# LEGGI ED ALTRI ATTI NORMATIVI

LEGGE 28 giugno 2024, n. **90**.

**Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.**

La Camera dei deputati ed il Senato della Repubblica hanno approvato;

IL PRESIDENTE DELLA REPUBBLICA

PROMULGA

la seguente legge:

## *Capo I*

DISPOSIZIONI IN MATERIA DI RAFFORZAMENTO DELLA CYBERSICUREZZA NAZIONALE, DI RESILIENZA DELLE PUBBLICHE AMMINISTRAZIONI E DEL SETTORE FINANZIARIO, DI PERSONALE E FUNZIONAMENTO DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE E DEGLI ORGANISMI DI INFORMAZIONE PER LA SICUREZZA NONCHÉ DI CONTRATTI PUBBLICI DI BENI E SERVIZI INFORMATICI IMPIEGATI IN UN CONTESTO CONNESSO ALLA TUTELA DEGLI INTERESSI NAZIONALI STRATEGICI

### Art. 1.

*Obblighi di notifica di incidenti*

1. Le pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, le regioni e le province autonome di Trento e di Bolzano, le città metropolitane, i comuni con popolazione superiore a 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e le aziende sanitarie locali segnalano e notificano, con le modalità e nei termini di cui al comma 2 del presente articolo, gli incidenti indicati nella tassonomia di cui all'articolo 1, comma 3-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, come modificato dall'articolo 3 della presente legge, aventi impatto su reti, sistemi informativi e servizi informatici. Tra i soggetti di cui al presente comma sono altresì comprese le rispettive società *in house* che forniscono servizi informatici, i servizi di trasporto di cui al primo periodo del presente comma ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008.

2. I soggetti di cui al comma 1 segnalano, senza ritardo e comunque entro il termine massimo di ventiquattro ore dal momento in cui ne sono venuti a conoscenza a seguito delle evidenze comunque ottenute, qualunque incidente riconducibile a una delle tipologie individuate nella tassonomia di cui al comma 1 ed effettuano, entro settantadue ore a decorrere dal medesimo momento, la notifica completa di tutti gli elementi informativi disponibili. La segnalazione e la successiva notifica sono effettuate tramite le apposite procedure disponibili nel sito *internet* istituzionale dell'Agenzia per la cybersicurezza nazionale.

3. Per i comuni con popolazione superiore a 100.000 abitanti e i comuni capoluoghi di regione, per le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, per le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane, per le aziende sanitarie locali e per le società *in house* che forniscono servizi informatici, i servizi di trasporto di cui al presente comma ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008, gli obblighi di cui ai commi 1 e 2 del presente articolo si applicano a decorrere dal centottantesimo giorno successivo alla data di entrata in vigore della presente legge.

4. Qualora i soggetti di cui al comma 1 effettuino notifiche volontarie di incidenti al di fuori dei casi indicati nella tassonomia di cui al medesimo comma 1, si applicano le disposizioni dell'articolo 18, commi 3, 4 e 5, del decreto legislativo 18 maggio 2018, n. 65.

5. Nel caso di inosservanza dell'obbligo di notifica di cui ai commi 1 e 2, l'Agenzia per la cybersicurezza nazionale comunica all'interessato che la reiterazione dell'inosservanza, nell'arco di cinque anni, comporterà l'applicazione delle disposizioni di cui al comma 6 e può disporre, nei dodici mesi successivi all'accertamento del ritardo o dell'omissione, l'invio di ispezioni, anche al fine di verificare l'attuazione, da parte dei soggetti interessati dall'incidente, di interventi di rafforzamento della resilienza agli stessi, direttamente indicati dall'Agenzia per la cybersicurezza nazionale ovvero previsti da apposite linee guida adottate dalla medesima Agenzia. Le modalità di tali ispezioni sono disciplinate con determinazione del direttore generale dell'Agenzia per la cybersicurezza nazionale, pubblicata nella *Gazzetta Ufficiale*.

6. Nei casi di reiterata inosservanza, nell'arco di cinque anni, dell'obbligo di notifica di cui ai commi 1 e 2, l'Agenzia per la cybersicurezza nazionale applica altresì, nel rispetto delle disposizioni dell'articolo 17, comma 4-*quater*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, introdotto dall'articolo 11 della presente legge, una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000 a carico dei soggetti di cui al comma 1 del presente articolo. La violazione delle disposizioni del comma 1 del presente articolo può costituire causa di responsabilità disciplinare e amministrativo-contabile per i funzionari e i dirigenti responsabili.

7. Fermi restando gli obblighi e le sanzioni, anche penali, previsti da altre norme di legge, le disposizioni del presente articolo non si applicano:

*a)* ai soggetti di cui all'articolo 3, comma 1, lettere *g)* e *i)*, del decreto legislativo 18 maggio 2018, n. 65, e a quelli di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;

*b)* agli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124.

Art. 2.

*Mancato o ritardato adeguamento a segnalazioni dell'Agenzia per la cybersicurezza nazionale*

1. I soggetti di cui all'articolo 1, comma 1, della presente legge e quelli di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, all'articolo 3, comma 1, lettere *g)* e *i)*, del decreto legislativo 18 maggio 2018, n. 65, e all'articolo 40, comma 3, alinea, del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259, in caso di segnalazioni puntuali dell'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità cui essi risultino potenzialmente esposti, provvedono, senza ritardo e comunque non oltre quindici giorni dalla comunicazione, all'adozione degli interventi risolutivi indicati dalla stessa Agenzia.

2. La mancata o ritardata adozione degli interventi risolutivi di cui al comma 1 del presente articolo comporta l'applicazione delle sanzioni di cui all'articolo 1, comma 6, salvo il caso in cui motivate esigenze di natura tecnico-organizzativa, tempestivamente comunicate all'Agenzia per la cybersicurezza nazionale, ne impediscano l'adozione o ne comportino il differimento oltre il termine indicato al medesimo comma 1 del presente articolo.

Art. 3.

*Norme di raccordo con le disposizioni del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*

1. All'articolo 1, comma 3-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, sono apportate le seguenti modificazioni:

*a)* il secondo periodo è sostituito dal seguente: «I medesimi soggetti provvedono a effettuare la segnalazione degli incidenti di cui al presente comma senza ritardo, comunque entro il termine massimo di ventiquattro ore, e ad effettuare la relativa notifica entro settantadue ore»;

*b)* dopo il quarto periodo è inserito il seguente: «Nei casi di reiterata inosservanza degli obblighi di notifica di cui al presente comma, si applica la sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000».

Art. 4.

*Disposizioni in materia di dati relativi a incidenti informatici*

1. All'articolo 7, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, dopo la lettera n-*bis*) è inserita la seguente:

«n-*ter*) provvede alla raccolta, all'elaborazione e alla classificazione dei dati relativi alle notifiche di incidenti ricevute dai soggetti che a ciò siano tenuti in osservanza delle disposizioni vigenti. Tali dati sono resi pubblici nell'ambito della relazione prevista dall'articolo 14, comma 1, quali dati ufficiali di riferimento degli attacchi informatici portati ai soggetti che operano nei settori rilevanti per gli interessi nazionali nel campo della cybersicurezza. Agli adempimenti previsti dalla presente lettera si provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente».

Art. 5.

*Disposizioni in materia di Nucleo per la cybersicurezza*

1. All'articolo 8 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, dopo il comma 4 è inserito il seguente:

«4.1. In relazione a specifiche questioni di particolare rilevanza concernenti i compiti di cui all'articolo 9, comma 1, lettera *a)*, il Nucleo può essere convocato nella composizione di cui al comma 4 del presente articolo, di volta in volta estesa alla partecipazione di un rappresentante della Direzione nazionale antimafia e antiterrorismo, della Banca d'Italia o di uno o più operatori di cui all'articolo 1, comma 2-*bis*, del decreto-legge perimetro, nonché di eventuali altri soggetti, interessati alle stesse questioni. Le amministrazioni e i soggetti convocati partecipano alle suddette riunioni a livello di vertice».

Art. 6.

*Disposizioni in materia di coordinamento operativo tra i servizi di informazione per la sicurezza e l'Agenzia per la cybersicurezza nazionale*

1. Qualora le Agenzie di cui agli articoli 6 e 7 della legge 3 agosto 2007, n. 124, avuta notizia di un evento o un incidente informatici, ritengano strettamente necessario, per il perseguimento delle finalità istituzionali del Sistema di informazione per la sicurezza della Repubblica, il differimento di una o più delle attività di resilienza di cui all'articolo 7, comma 1, lettere *n)* e n-*bis*), del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, le predette Agenzie, per il tramite del Dipartimento delle informazioni per la sicurezza (DIS), ne informano il Presidente del Consiglio dei ministri o l'Autorità delegata di cui all'articolo 3 della citata legge n. 124 del 2007, ove istituita.

2. Nei casi di cui al comma 1, il Presidente del Consiglio dei ministri, sentiti il direttore generale del Dipartimento delle informazioni per la sicurezza e il direttore generale dell'Agenzia per la cybersicurezza nazionale, può

disporre il differimento degli obblighi informativi cui è in ogni caso tenuta l'Agenzia ai sensi delle disposizioni vigenti, ivi compresi quelli previsti ai sensi dell'articolo 17, commi 4 e 4-*bis*, del decreto-legge n. 82 del 2021, nonché il differimento di una o più delle attività di resilienza di cui all'articolo 7, comma 1, lettere *n)* e n-*bis*), del medesimo decreto-legge.

Art. 7.

*Composizione del Comitato interministeriale per la sicurezza della Repubblica*

1. All'articolo 5, comma 3, della legge 3 agosto 2007, n. 124, sono apportate le seguenti modificazioni:

*a)* dopo le parole: «Ministro degli affari esteri» sono inserite le seguenti: «e della cooperazione internazionale»;

*b)* le parole: «dello sviluppo economico e dal Ministro della transizione ecologica» sono sostituite dalle seguenti: «delle imprese e del made in Italy, dal Ministro dell'ambiente e della sicurezza energetica, dal Ministro dell'agricoltura, della sovranità alimentare e delle foreste, dal Ministro delle infrastrutture e dei trasporti e dal Ministro dell'università e della ricerca».

Art. 8.

*Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza*

1. I soggetti di cui all'articolo 1, comma 1, individuano, ove non sia già presente, una struttura, anche tra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, che provvede:

*a)* allo sviluppo delle politiche e delle procedure di sicurezza delle informazioni;

*b)* alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico;

*c)* alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione;

*d)* alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione;

*e)* alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere *b)* e *d)*;

*f)* alla pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale;

*g)* al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.

2. Presso le strutture di cui al comma 1 opera il referente per la cybersicurezza, individuato in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza. Qualora i soggetti di cui all'articolo 1, comma 1, non dispongano di personale dipendente fornito di tali requisiti, possono conferire l'incarico di referente per la cybersicurezza a un dipendente di una pubblica amministrazione, previa autorizzazione di quest'ultima ai sensi dell'articolo 53 del decreto legislativo 30 marzo 2001, n. 165, nell'ambito delle risorse disponibili a legislazione vigente. Il referente per la cybersicurezza svolge anche la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale in relazione a quanto previsto dalla presente legge e dalle normative settoriali in materia di cybersicurezza cui è soggetta la medesima amministrazione. A tale fine, il nominativo del referente per la cybersicurezza è comunicato all'Agenzia per la cybersicurezza nazionale.

3. La struttura e il referente di cui ai commi 1 e 2 possono essere individuati, rispettivamente, nell'ufficio e nel responsabile per la transizione al digitale previsti dall'articolo 17 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82.

4. I compiti di cui ai commi 1 e 2 possono essere esercitati in forma associata secondo quanto previsto dall'articolo 17, commi 1-*sexies* e 1-*septies*, del codice di cui al decreto legislativo 7 marzo 2005, n. 82.

5. L'Agenzia per la cybersicurezza nazionale può individuare modalità e processi di coordinamento e di collaborazione tra le amministrazioni di cui all'articolo 1, comma 1, e tra i referenti per la cybersicurezza di cui al comma 2 del presente articolo, al fine di facilitare la resilienza delle amministrazioni pubbliche.

6. Le disposizioni del presente articolo non si applicano:

*a)* ai soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, ai quali continuano ad applicarsi gli obblighi previsti dalle disposizioni di cui alla richiamata disciplina;

*b)* agli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124.

Art. 9.

*Rafforzamento delle misure di sicurezza dei dati attraverso la crittografia*

1. Le strutture di cui all'articolo 8 della presente legge nonché quelle che svolgono analoghe funzioni per i soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e al decreto legislativo 18 maggio 2018, n. 65, verificano che i programmi e le applicazioni informatiche e di comunicazione elettronica in uso, che utilizzano soluzioni crittografiche, rispettino le linee guida sulla crittografia nonché quelle sulla conservazione delle *password* adottate dall'Agenzia per la cybersicurezza nazionale e dal Garante per la protezione dei dati personali e non comportino vulnerabilità note, atte a rendere disponibili e intellegibili a terzi i dati cifrati.

Art. 10.

*Funzioni dell'Agenzia per la cybersicurezza nazionale in materia di crittografia*

1. All'articolo 7, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, la lettera m-*bis*) è sostituita dalla seguente:

«m-*bis*) provvede, anche attraverso un'apposita sezione nell'ambito della strategia di cui alla lettera *b)*, allo sviluppo e alla diffusione di *standard*, linee guida e raccomandazioni al fine di rafforzare la cybersicurezza dei sistemi informatici, alla valutazione della sicurezza dei sistemi crittografici nonché all'organizzazione e alla gestione di attività di divulgazione finalizzate a promuovere l'utilizzo della crittografia, anche a vantaggio della tecnologia *blockchain*, come strumento di cybersicurezza. L'Agenzia, anche per il rafforzamento dell'autonomia industriale e tecnologica dell'Italia, promuove altresì la collaborazione con centri universitari e di ricerca per la valorizzazione dello sviluppo di nuovi algoritmi proprietari, la ricerca e il conseguimento di nuove capacità crittografiche nazionali nonché la collaborazione internazionale con gli organismi esteri che svolgono analoghe funzioni. A tale fine, è istituito presso l'Agenzia, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, il Centro nazionale di crittografia, il cui funzionamento è disciplinato con provvedimento del direttore generale dell'Agenzia stessa. Il Centro nazionale di crittografia svolge le funzioni di centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato, ferme restando le competenze dell'Ufficio centrale per la segretezza, di cui all'articolo 9 della legge 3 agosto 2007, n. 124, con riferimento alle informazioni e alle attività previste dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della citata legge n. 124 del 2007, nonché le competenze degli organismi di cui agli articoli 4, 6 e 7 della medesima legge».

Art. 11.

*Procedimento amministrativo sanzionatorio per l'accertamento e la contestazione delle violazioni in materia di cybersicurezza di competenza dell'Agenzia per la cybersicurezza nazionale*

1. All'articolo 17 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, dopo il comma 4-*ter* è inserito il seguente:

«4-*quater*. La disciplina del procedimento sanzionatorio amministrativo dell'Agenzia è definita con regolamento che stabilisce, in particolare, termini e modalità per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia ai sensi del presente decreto e delle altre disposizioni che assegnano poteri accertativi e sanzionatori all'Agenzia. Il regolamento di cui al primo periodo è adottato, entro novanta giorni dalla data di entrata in vigore della presente disposizione, con decreto del Presidente del Consiglio dei ministri, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, sentito il Comitato interministeriale per la cybersicurezza e acquisito il parere delle competenti Commissioni parlamentari. Fino alla data di entrata in vigore del regolamento di cui al presente comma, ai procedimenti sanzionatori si applicano, per ciascuna fase procedimentale di cui al primo periodo, le disposizioni contenute nelle sezioni I e II del capo I della legge 24 novembre 1981, n. 689».

Art. 12.

*Disposizioni in materia di personale dell'Agenzia per la cybersicurezza nazionale*

1. All'articolo 12 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, dopo il comma 8-*bis* è aggiunto il seguente:

«8-*ter*. I dipendenti appartenenti al ruolo del personale dell'Agenzia di cui al comma 2, lettera *a)*, che abbiano partecipato, nell'interesse e a spese dell'Agenzia, a specifici percorsi formativi di specializzazione, per la durata di due anni a decorrere dalla data di completamento dell'ultimo dei predetti percorsi formativi non possono essere assunti né assumere incarichi presso soggetti privati al fine di svolgere mansioni in materia di cybersicurezza. I contratti stipulati in violazione di quanto disposto dal presente comma sono nulli. Le disposizioni del presente comma non si applicano al personale cessato dal servizio presso l'Agenzia secondo quanto previsto dalle disposizioni del regolamento adottato ai sensi del presente articolo relative al collocamento a riposo d'ufficio, al raggiungimento del requisito anagrafico previsto dalla legge per la pensione di vecchiaia, alla cessazione a domanda per inabilità o alla dispensa dal servizio per motivi di salute. I percorsi formativi di specializzazione di cui al presente comma sono individuati con determinazione del direttore generale dell'Agenzia, tenendo conto della particolare qualità dell'offerta formativa, dei costi, della durata e del livello di specializzazione che consegue alla frequenza dei suddetti percorsi».

2. Fino al 31 dicembre 2026, per il personale dell'Agenzia per la cybersicurezza nazionale il requisito di permanenza minima nell'Area operativa ai fini del passaggio all'Area manageriale e alte professionalità è fissato in tre anni.

Art. 13.

*Disposizioni in materia di personale degli organismi di informazione per la sicurezza*

1. Coloro che hanno ricoperto la carica di direttore generale e di vice direttore generale del DIS e di direttore e di vice direttore dell'Agenzia informazioni e sicurezza esterna (AISE) o dell'Agenzia informazioni e sicurezza interna (AISI) ovvero hanno svolto incarichi dirigenziali di prima fascia di preposizione a strutture organizzative di livello dirigenziale generale non possono, salva autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità delegata, ove istituita, nei tre anni successivi alla cessazione dall'incarico, svolgere attività lavorativa, professionale o di consulenza né ricoprire cariche presso

soggetti esteri, pubblici o privati, ovvero presso soggetti privati italiani a cui si applica il decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56. L'autorizzazione è concessa tenendo conto delle esigenze di protezione e di tutela del patrimonio informativo acquisito durante l'espletamento dell'incarico e della necessità di evitare comunque pregiudizi per la sicurezza nazionale.

2. Il personale appartenente al ruolo unico previsto dall'articolo 21 della legge 3 agosto 2007, n. 124, non può, nei tre anni successivi alla cessazione dal servizio presso il DIS, l'AISE e l'AISI, svolgere attività lavorativa, professionale o di consulenza né ricoprire cariche presso enti o privati titolari di licenza ai sensi dell'articolo 134 del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773, o comunque presso soggetti che a qualunque titolo svolgano attività di investigazione, ricerca o raccolta informativa.

3. Il personale appartenente al ruolo unico previsto dall'articolo 21 della legge 3 agosto 2007, n. 124, che abbia partecipato, nell'interesse e a spese del DIS, dell'AISE o dell'AISI, a specifici percorsi formativi di specializzazione, per la durata di tre anni a decorrere dalla data di completamento dell'ultimo dei predetti percorsi formativi non può essere assunto né assumere incarichi presso soggetti privati per svolgere le medesime mansioni per le quali ha beneficiato delle suddette attività formative.

4. I contratti stipulati e gli incarichi conferiti in violazione dei divieti di cui al presente articolo sono nulli.

5. Con regolamento adottato ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124, sono definiti le procedure di autorizzazione per i casi di cui al comma 1, gli obblighi di dichiarazione e di comunicazione a carico dei dipendenti, i casi in cui non si applicano i divieti di cui ai commi 2 e 3 e le modalità di individuazione dei percorsi formativi che determinano il divieto di cui al comma 3.

Art. 14.

*Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e disposizioni di raccordo con il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*

1. Con decreto del Presidente del Consiglio dei ministri, da adottare entro centoventi giorni dalla data di entrata in vigore della presente legge, su proposta dell'Agenzia per la cybersicurezza nazionale, previo parere del Comitato interministeriale per la sicurezza della Repubblica, di cui all'articolo 5 della legge 3 agosto 2007, n. 124, nella composizione di cui all'articolo 10, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, sono individuati, per specifiche categorie tecnologiche di beni e servizi informatici, gli elementi essenziali di cybersicurezza che i soggetti di cui all'articolo 2, comma 2, del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, tengono in considerazione nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici nonché i casi in cui, per la tutela della sicurezza nazionale, devono essere previsti criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi individuati con il decreto di cui al presente comma tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione. Ai fini del presente articolo, si intende per «elementi essenziali di cybersicurezza» l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela di cui al primo periodo.

2. Nei casi individuati ai sensi del comma 1, le stazioni appaltanti, comprese le centrali di committenza:

*a)* possono esercitare la facoltà di cui agli articoli 107, comma 2, e 108, comma 10, del codice dei contratti pubblici, di cui al decreto legislativo 31 marzo 2023, n. 36, se accertano che l'offerta non tiene in considerazione gli elementi essenziali di cybersicurezza individuati con il decreto di cui al comma 1;

*b)* tengono sempre in considerazione gli elementi essenziali di cybersicurezza di cui al comma 1 nella valutazione dell'elemento qualitativo, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione;

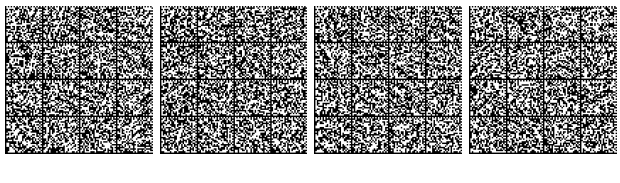
*c)* nel caso in cui sia utilizzato il criterio del minor prezzo, ai sensi dell'articolo 108, comma 3, del codice di cui al decreto legislativo n. 36 del 2023, inseriscono gli elementi di cybersicurezza di cui al comma 1 del presente articolo tra i requisiti minimi dell'offerta;

*d)* nel caso in cui sia utilizzato il criterio dell'offerta economicamente più vantaggiosa, ai sensi dell'articolo 108, comma 4, del codice di cui al decreto legislativo n. 36 del 2023, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del migliore rapporto qualità/prezzo, stabiliscono un tetto massimo per il punteggio economico entro il limite del 10 per cento;

*e)* prevedono criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti alla NATO o di Paesi terzi individuati con il decreto di cui al comma 1 tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione, al fine di tutelare la sicurezza nazionale e di conseguire l'autonomia tecnologica e strategica nell'ambito della cybersicurezza.

3. Le disposizioni di cui al comma 1 si applicano anche ai soggetti privati non compresi tra quelli di cui all'articolo 2, comma 2, del codice di cui al decreto legislativo 7 marzo 2005, n. 82, e inseriti nell'elencazione di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.





4. Resta fermo quanto stabilito dall'articolo 1 del citato decreto-legge n. 105 del 2019 per i casi ivi previsti di approvvigionamento di beni, sistemi e servizi di *information and communication technology* destinati ad essere impiegati nelle reti e nei sistemi informativi nonché per l'espletamento dei servizi informatici di cui alla lettera *b)* del comma 2 del medesimo articolo 1.

Art. 15.

*Modifica all'articolo 16 della legge 21 febbraio 2024, n. 15*

1. All'articolo 16, comma 2, della legge 21 febbraio 2024, n. 15, dopo la lettera *c)* è inserita la seguente:

«*c*-bis) apportare alla disciplina applicabile agli intermediari finanziari iscritti nell'albo previsto dall'articolo 106 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, nonché alla società Poste italiane Spa per l'attività del Patrimonio Bancoposta, di cui al regolamento di cui al decreto del Presidente della Repubblica 14 marzo 2001, n. 144, le occorrenti modifiche e integrazioni, anche mediante la normativa secondaria di cui alla lettera *d)* del presente comma, per conseguire un livello elevato di resilienza operativa digitale e assicurare la stabilità del settore finanziario nel suo complesso, in particolare:

1) definendo presìdi in materia di resilienza operativa digitale equivalenti a quelli stabiliti nel regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022;

2) tenendo conto, nella definizione dei presìdi di cui al numero 1), del principio di proporzionalità e delle attività svolte dagli intermediari finanziari e dal Patrimonio Bancoposta;

3) attribuendo alla Banca d'Italia l'esercizio dei poteri di vigilanza, di indagine e sanzionatori di cui alla lettera *b)* nei confronti dei soggetti di cui alla presente lettera».

*Capo II*

DISPOSIZIONI PER LA PREVENZIONE E IL CONTRASTO DEI REATI INFORMATICI NONCHÉ IN MATERIA DI COORDINAMENTO DEGLI INTERVENTI IN CASO DI ATTACCHI A SISTEMI INFORMATICI O TELEMATICI E DI SICUREZZA DELLE BANCHE DI DATI IN USO PRESSO GLI UFFICI GIUDIZIARI

Art. 16.

*Modifiche al codice penale*

1. Al codice penale sono apportate le seguenti modificazioni:

*a)* all'articolo 240, secondo comma, numero 1-*bis*, dopo la parola: «635-*quinquies*,» sono inserite le seguenti: «640, secondo comma, numero 2-*ter*),»;

*b)* all'articolo 615-*ter*:

1) al secondo comma:

1.1) all'alinea, le parole: «da uno a cinque anni» sono sostituite dalle seguenti: «da due a dieci anni»;

1.2) al numero 2), dopo la parola: «usa» sono inserite le seguenti: «minaccia o»;

1.3) al numero 3), dopo le parole: «ovvero la distruzione o il danneggiamento» sono inserite le seguenti: «ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare»;

2) al terzo comma, le parole: «da uno a cinque anni e da tre a otto anni» sono sostituite dalle seguenti: «da tre a dieci anni e da quattro a dodici anni»;

*c)* all'articolo 615-*quater*:

1) al primo comma, la parola: «profitto» è sostituita dalla seguente: «vantaggio»;

2) il secondo comma è sostituito dal seguente:

«La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-*ter*, secondo comma, numero 1)»;

3) dopo il secondo comma è aggiunto il seguente:

«La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-*ter*, terzo comma»;

*d)* l'articolo 615-*quinquies* è abrogato;

*e)* all'articolo 617-*bis*:

1) dopo il primo comma è inserito il seguente:

«La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-*ter*, secondo comma, numero 1)»;

2) al secondo comma, le parole da:

«ovvero da un pubblico ufficiale» fino alla fine del comma sono soppresse;

*f)* all'articolo 617-*quater*, quarto comma:

1) all'alinea, le parole: «da tre a otto anni» sono sostituite dalle seguenti: «da quattro a dieci anni»;

2) il numero 1) è sostituito dal seguente:

«1) in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615-*ter*, terzo comma»;

3) al numero 2), le parole: «da un pubblico ufficiale» sono sostituite dalle seguenti: «in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o da un pubblico ufficiale» e la parola: «ovvero» è sostituita dalle seguenti: «o da chi esercita, anche abusivamente, la professione di investigatore privato, o»;

4) il numero 3) è abrogato;

*g)* all'articolo 617-*quinquies*:

1) il secondo comma è sostituito dal seguente:

«Quando ricorre taluna delle circostanze di cui all'articolo 617-*quater*, quarto comma, numero 2), la pena è della reclusione da due a sei anni»;

2) dopo il secondo comma è aggiunto il seguente:

«Quando ricorre taluna delle circostanze di cui all'articolo 617-*quater*, quarto comma, numero 1), la pena è della reclusione da tre a otto anni»;

*h)* all'articolo 617-*sexies*, secondo comma, le parole: «da uno a cinque anni» sono sostituite dalle seguenti: «da tre a otto anni»;

*i)* alla rubrica del capo III-*bis* del titolo dodicesimo del libro secondo, le parole:

«sulla procedibilità» sono soppresse;

*l)* nel capo III-*bis* del titolo dodicesimo del libro secondo, dopo l'articolo 623-*ter* è aggiunto il seguente:

«Art. 623-*quater (Circostanze attenuanti)*. — Le pene comminate per i delitti di cui agli articoli 615-*ter*, 615-*quater*, 617-*quater*, 617-*quinquies* e 617-*sexies* sono diminuite quando, per la natura, la specie, i mezzi, le modalità o le circostanze dell'azione ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità.

Le pene comminate per i delitti di cui al primo comma sono diminuite dalla metà a due terzi per chi si adopera per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi.

Non si applica il divieto di cui all'articolo 69, quarto comma»;

*m)* all'articolo 629:

1) al secondo comma, le parole: «nell'ultimo capoverso dell'articolo precedente» sono sostituite dalle seguenti: «nel terzo comma dell'articolo 628»;

2) dopo il secondo comma è aggiunto il seguente:

«Chiunque, mediante le condotte di cui agli articoli 615-*ter*, 617-*quater*, 617-*sexies*, 635-*bis*, 635-*quater* e 635-*quinquies* ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità»;

*n)* all'articolo 635-*bis*:

1) al primo comma, le parole: «da sei mesi a tre anni» sono sostituite dalle seguenti: «da due a sei anni»;

2) il secondo comma è sostituito dal seguente:

«La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato»;

*o)* all'articolo 635-*ter*:

1) al primo comma, le parole: «utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni» sono sostituite dalle seguenti: «di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, è punito con la reclusione da due a sei anni»;

2) il secondo e il terzo comma sono sostituiti dai seguenti:

«La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.

La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3)»;

3) nella rubrica, le parole: «utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità» sono sostituite dalle seguenti: «pubblici o di interesse pubblico»;

*p)* all'articolo 635-*quater*:

1) al primo comma, le parole: «da uno a cinque anni» sono sostituite dalle seguenti: «da due a sei anni»;

2) il secondo comma è sostituito dal seguente:

«La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato»;

*q)* dopo l'articolo 635-*quater* è inserito il seguente:

«Art. 635-*quater*.1 *(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 ovvero 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 fino a euro 10.329.

La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-*ter*, secondo comma, numero 1).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-*ter*, terzo comma»;

*r)* l'articolo 635-*quinquies* è sostituito dal seguente:

«Art. 635-*quinquies (Danneggiamento di sistemi informatici o telematici di pubblico interesse)*. — Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-*bis* ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, compie atti diretti a distruggere, danneggiare o rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento è punito con la pena della reclusione da due a sei anni.

La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.

La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3)»;

*s)* nel capo I del titolo tredicesimo del libro secondo, dopo l'articolo 639-*bis* è aggiunto il seguente:

«Art. 639-*ter (Circostanze attenuanti)*. — Le pene comminate per i delitti di cui agli articoli 629, terzo comma, 635-*ter*, 635-*quater*.1 e 635-*quinquies* sono diminuite quando, per la natura, la specie, i mezzi, le modalità o le circostanze dell'azione ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità.

Le pene comminate per i delitti di cui al primo comma sono diminuite dalla metà a due terzi per chi si adopera per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi.

Non si applica il divieto di cui all'articolo 69, quarto comma»;

*t)* all'articolo 640:

1) al secondo comma è aggiunto, in fine, il seguente numero:

«2-*ter*) se il fatto è commesso a distanza attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione»;

2) al terzo comma, le parole: «capoverso precedente» sono sostituite dalle seguenti: «secondo comma, a eccezione di quella di cui al numero 2-*ter*)»;

*u)* all'articolo 640-*quater*, le parole: «numero 1» sono sostituite dalle seguenti: «numeri 1 e 2-*ter*)».

Art. 17.

*Modifiche al codice di procedura penale*

1. Al codice di procedura penale sono apportate le seguenti modificazioni:

*a)* all'articolo 51, comma 3-*quinquies*:

1) la parola: «615-*quinquies*,» è soppressa;

2) dopo la parola: «635-*quater*,» sono inserite le seguenti: «635-*quater*.1, 635-*quinquies*,»;

3) dopo le parole: «del codice penale,» sono inserite le seguenti: «o per il delitto di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133,»;

*b)* all'articolo 406, comma 5-*bis*, le parole: «numeri 4 e 7-*bis*» sono sostituite dalle seguenti: «numeri 4), 7-*bis*) e 7-*ter*)»;

*c)* all'articolo 407, comma 2, lettera *a)*, dopo il numero 7-*bis*) è aggiunto il seguente:

«7-*ter*) delitti previsti dagli articoli 615-*ter*, 615-*quater*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, 635-*quater*.1 e 635-*quinquies* del codice penale, quando il fatto è commesso in danno di 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».

Art. 18.

*Modifiche al decreto-legge 15 gennaio 1991, n. 8, convertito, con modificazioni, dalla legge 15 marzo 1991, n. 82*

1. Al decreto-legge 15 gennaio 1991, n. 8, convertito, con modificazioni, dalla legge 15 marzo 1991, n. 82, sono apportate le seguenti modificazioni:

*a)* all'articolo 9, comma 2, dopo le parole: «51, comma 3-*bis*,» sono inserite le seguenti: «o all'articolo 371-*bis*, comma 4-*bis*,»;

*b)* all'articolo 11, comma 2, dopo le parole: «51, commi 3-*bis* e 3-*quater*,» sono inserite le seguenti: «o all'articolo 371-*bis*, comma 4-*bis*,»;

*c)* all'articolo 16-*nonies*, comma 1, dopo le parole: «51, comma 3-*bis*,» sono inserite le seguenti: «o all'articolo 371-*bis*, comma 4-*bis*,».

Art. 19.

*Modifica al decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203*

1. All'articolo 13 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, dopo il comma 3 è aggiunto il seguente:

«3-*bis*. Le disposizioni dei commi 1, 2 e 3 si applicano anche quando si procede in relazione a taluno dei delitti, consumati o tentati, previsti dall'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale».

Art. 20.

*Modifiche al decreto legislativo 8 giugno 2001, n. 231*

1. All'articolo 24-*bis* del decreto legislativo 8 giugno 2001, n. 231, sono apportate le seguenti modificazioni:

*a)* al comma 1, le parole: «da cento a cinquecento quote» sono sostituite dalle seguenti: «da duecento a settecento quote»;

*b)* dopo il comma 1 è inserito il seguente:

«1-*bis*. In relazione alla commissione del delitto di cui all'articolo 629, terzo comma, del codice penale, si applica all'ente la sanzione pecuniaria da trecento a ottocento quote»;

*c)* al comma 2, la parola: «615-*quinquies*» è sostituita dalla seguente: «635-*quater*.1» e le parole: «sino a trecento quote» sono sostituite dalle seguenti: «sino a quattrocento quote»;

*d)* al comma 4, dopo il primo periodo è inserito il seguente: «Nei casi di condanna per il delitto indicato nel comma 1-*bis* si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a due anni».

Art. 21.

*Modifica alla legge 11 gennaio 2018, n. 6*

1. All'articolo 11, comma 2, della legge 11 gennaio 2018, n. 6, dopo le parole: «51, commi 3-*bis*, 3-*ter* e 3-*quater*,» sono inserite le seguenti: «o all'articolo 371-*bis*, comma 4-*bis*,».

Art. 22.

*Modifiche al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109*

1. All'articolo 17 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, sono apportate le seguenti modificazioni:

*a)* il comma 4 è sostituito dal seguente:

«4. Il personale dell'Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni, riveste la qualifica di pubblico ufficiale. La trasmissione immediata delle notifiche di incidente ricevute dal CSIRT Italia all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, costituisce adempimento dell'obbligo di cui all'articolo 331 del codice di procedura penale»;

*b)* dopo il comma 4-*bis* sono inseriti i seguenti:

«4-*bis*.1. Nei casi in cui l'Agenzia ha notizia di un attacco ai danni di uno dei sistemi informatici o telematici di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale e in ogni caso quando risulti interessato taluno dei soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge perimetro, all'articolo 3, comma 1, lettere *g)* e *i)*, del decreto legislativo NIS ovvero all'articolo 40, comma 3, alinea, del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259, fermo restando quanto previsto dal comma 4 del presente articolo, procede alle attività di cui all'articolo 7, comma 1, lettere *n)* e n-*bis*), e ne informa senza ritardo il procuratore nazionale antimafia e antiterrorismo, ai sensi del comma 4-*bis* del presente articolo.

4-*bis*.2. Fuori dei casi di cui al comma 4-*bis*.1, quando acquisisce la notizia dei delitti di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale, il pubblico ministero ne dà tempestiva informazione all'Agenzia e assicura, altresì, il raccordo informativo con l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione ai fini di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

4-*bis*.3. In ogni caso, il pubblico ministero impartisce le disposizioni necessarie ad assicurare che gli accertamenti urgenti siano compiuti tenendo conto delle attività svolte dall'Agenzia, a fini di resilienza, di cui all'articolo 7, comma 1, lettere *n)* e n-*bis*), e può disporre il differimento di una o più delle predette attività, con provvedimento motivato adottato senza ritardo, per evitare un grave pregiudizio per il corso delle indagini.

4-*bis*.4. Il pubblico ministero, quando procede ad accertamenti tecnici irripetibili in relazione ai delitti di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale, informa senza ritardo l'Agenzia, che mediante propri rappresentanti può assistere al conferimento dell'incarico e partecipare agli accertamenti. Le disposizioni del primo periodo si applicano anche quando agli accertamenti si procede nelle forme dell'incidente probatorio».

Art. 23.

*Modifiche all'articolo 7 della legge 12 agosto 1962, n. 1311*

1. All'articolo 7 della legge 12 agosto 1962, n. 1311, sono apportate le seguenti modificazioni:

*a)* al primo comma è aggiunto, in fine, il seguente periodo: «Nelle ispezioni è verificato altresì il rispetto delle prescrizioni di sicurezza negli accessi alle banche di dati in uso presso gli uffici giudiziari»;

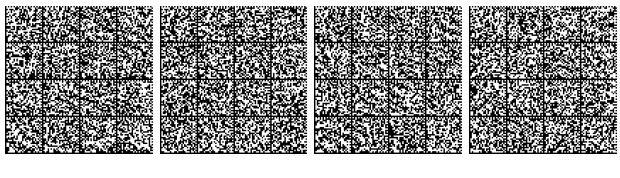
*b)* al terzo comma, le parole: «degli stessi nonché» sono sostituite dalle seguenti: «degli stessi,» e sono aggiunte, in fine, le seguenti parole: «nonché il rispetto delle prescrizioni di sicurezza negli accessi alle banche di dati in uso presso gli uffici giudiziari».

Art. 24.

*Disposizioni finanziarie*

1. Dall'attuazione della presente legge non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni pubbliche competenti provvedono all'adempimento dei compiti derivanti dalla presente legge con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.





2. I proventi delle sanzioni di cui all'articolo 1, comma 6, della presente legge confluiscono nelle entrate dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 11, comma 2, lettera *f)*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

La presente legge, munita del sigillo dello Stato, sarà inserita nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarla e di farla osservare come legge dello Stato.

Data a Roma, addì 28 giugno 2024

MATTARELLA

MELONI, *Presidente del Consiglio dei ministri*

NORDIO, *Ministro della giustizia*

Visto, *il Guardasigilli:* NORDIO

---

LAVORI PREPARATORI

*Camera dei deputati* (atto n. 1717):

Presentato dal Presidente del Consiglio dei ministri Giorgia MELONI e dal Ministro della giustizia Carlo NORDIO (Governo MELONI-I), il 16 febbraio 2024.

Assegnato alle Commissioni riunite I (Affari costituzionali, della Presidenza del Consiglio e interni) e II (Giustizia), in sede referente, il 29 febbraio 2024, con i pareri delle Commissioni IV (Difesa), V (Bilancio, tesoro e programmazione),VI (Finanze), VIII (Ambiente, territorio e lavori pubblici), IX (Trasporti, Poste e Telecomunicazioni), X (Attività produttive, commercio e turismo), XI (Lavoro pubblico e privato), XII (Affari sociali), XIV (Politiche dell'Unione europea) e per le Questioni regionali.

Esaminato dalle Commissioni riunite I (Affari costituzionali, della Presidenza del Consiglio e interni) e II (Giustizia), in sede referente, il 13 e il 19 marzo 2024; il 9, il 23 e il 24 aprile 2024; il 7 e l'8 maggio 2024.

Esaminato in Aula il 13 e 14 maggio 2024 e approvato il 15 maggio 2024.

*Senato della Repubblica* (atto n. 1143):

Assegnato alle Commissioni riunite 1ª (Affari costituzionali, affari della Presidenza del Consiglio e dell'Interno, ordinamento generale dello Stato e della pubblica amministrazione, editoria, digitalizzazione) e 2ª (Giustizia), in sede referente, il 20 maggio 2024, con i pareri delle Commissioni 3ª (Affari esteri e difesa), 4ª Commissione (Politiche dell'Unione europea), 5ª (Programmazione economica, bilancio), 6ª (Finanze e tesoro), 7ª (Cultura e patrimonio culturale, istruzione pubblica, ricerca scientifica, spettacolo e sport), 8ª (Ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica), 9ª (Industria, commercio, turismo, agricoltura e produzione agroalimentare), 10ª (Affari sociali, sanità, lavoro pubblico e privato, previdenza sociale) e per le Questioni regionali.

Esaminato dalle Commissioni riunite 1ª (Affari costituzionali, affari della Presidenza del Consiglio e dell'Interno, ordinamento generale dello Stato e della pubblica amministrazione, editoria, digitalizzazione) e 2ª (Giustizia), in sede referente, il 23 e il 29 maggio 2024; il 12 giugno 2024.

Esaminato in Aula e approvato definitivamente il 19 giugno 2024.

---

NOTE

AVVERTENZA:

Il testo delle note qui pubblicato è stato redatto dall'amministrazione competente per materia, ai sensi dell'art.10, commi 2 e 3, del testo unico delle disposizioni sulla promulgazione delle leggi, sull'emanazione dei decreti del Presidente della Repubblica e sulle pubblicazioni ufficiali della Repubblica italiana, approvato con d.p.r. 28 dicembre 1985, n.1092, al solo fine di facilitare la lettura delle disposizioni di legge modificate o alle quali è operato il rinvio. Restano invariati il valore e l'efficacia degli atti legislativi qui trascritti.

Per le direttive CEE vengono forniti gli estremi di pubblicazione nella *Gazzetta Ufficiale* delle comunità europee (GUUE).

*Note all'art. 1:*

— Si riporta l'articolo 1 della legge 31 dicembre 2009, n. 196 (Legge di contabilità e finanza pubblica):

«Art. 1 *(Princìpi di coordinamento e ambito di riferimento)*. — 1. Le amministrazioni pubbliche concorrono al perseguimento degli obiettivi di finanza pubblica definiti in ambito nazionale in coerenza con le procedure e i criteri stabiliti dall'Unione europea e ne condividono le conseguenti responsabilità. Il concorso al perseguimento di tali obiettivi si realizza secondo i principi fondamentali dell'armonizzazione dei bilanci pubblici e del coordinamento della finanza pubblica.

2. Ai fini della applicazione delle disposizioni in materia di finanza pubblica, per amministrazioni pubbliche si intendono, per l'anno 2011, gli enti e i soggetti indicati a fini statistici nell'elenco oggetto del comunicato dell'Istituto nazionale di statistica (ISTAT) in data 24 luglio 2010, pubblicato in pari data nella *Gazzetta Ufficiale* della Repubblica italiana n. 171, nonché a decorrere dall'anno 2012 gli enti e i soggetti indicati a fini statistici dal predetto Istituto nell'elenco oggetto del comunicato del medesimo Istituto in data 30 settembre 2011, pubblicato in pari data nella *Gazzetta Ufficiale* della Repubblica italiana n. 228, e successivi aggiornamenti ai sensi del comma 3 del presente articolo, effettuati sulla base delle definizioni di cui agli specifici regolamenti dell'Unione europea, le Autorità indipendenti e, comunque, le amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni.

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.

4. Le disposizioni recate dalla presente legge e dai relativi decreti legislativi costituiscono princìpi fondamentali del coordinamento della finanza pubblica ai sensi dell'articolo 117 della Costituzione e sono finalizzate alla tutela dell'unità economica della Repubblica italiana, ai sensi dell'articolo 120, secondo comma, della Costituzione.

5. Le disposizioni della presente legge si applicano alle regioni a statuto speciale e alle province autonome di Trento e di Bolzano nel rispetto di quanto previsto dai relativi statuti.».

— Si riporta l'articolo 1 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), convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, come modificato dalla presente legge:

«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. 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.

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.

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

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

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

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

1) alla struttura organizzativa preposta alla gestione della sicurezza;

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

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

3) alla protezione fisica e logica e dei dati;

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

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

6) al monitoraggio, test e controllo;

7) alla formazione e consapevolezza;

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

3-*bis*. Al di fuori dei casi di cui al comma 3, i soggetti di cui al comma 2-*bis* notificano gli incidenti di cui all'articolo 1, comma 1, lettera *h)*, del regolamento di cui al decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, aventi impatto su reti, sistemi informativi e servizi informatici di propria pertinenza diversi da quelli di cui al comma 2, lettera *b)*, del presente articolo, fatta eccezione per quelli aventi impatto sulle reti, sui sistemi informativi e sui servizi informatici del Ministero della difesa, per i quali si applicano i princìpi e le modalità di cui all'articolo 528, comma 1, lettera *d)*, del codice di cui al decreto legislativo 15 marzo 2010, n. 66. *I medesimi soggetti provvedono a effettuare la segnalazione degli incidenti di cui al presente comma senza ritardo, comunque entro il termine massimo di ventiquattro ore, e ad effettuare la relativa notifica entro settantadue ore*. Si applicano, altresì, le disposizioni di cui all'articolo 4, commi 2 e 4, del medesimo regolamento. Con determinazioni tecniche del direttore generale, sentito il vice direttore generale, dell'Agenzia per la cybersicurezza nazionale, è indicata la tassonomia degli incidenti che debbono essere oggetto di notifica ai sensi del presente comma e possono essere dettate specifiche modalità di notifica. *Nei casi di reiterata inosservanza degli obblighi di notifica di cui al presente comma, si applica la sanzione amministrativa pecuniaria da euro 25.000 a euro125.000.*

4. All'elaborazione delle misure di cui al comma 3, lettera *b)*, provvedono, secondo gli ambiti di competenza delineati dal presente decreto, il Ministero dello sviluppo economico e la Presidenza del Consiglio dei ministri, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e delle finanze e il Dipartimento delle informazioni per la sicurezza.

4-*bis*. Gli schemi dei decreti di cui ai commi 2 e 3 sono trasmessi alla Camera dei deputati e al Senato della Repubblica per l'espressione del parere delle Commissioni parlamentari competenti per materia, che si pronunciano nel termine di trenta giorni, decorso il quale il decreto può essere comunque adottato. I medesimi schemi sono altresì trasmessi al Comitato parlamentare per la sicurezza della Repubblica.

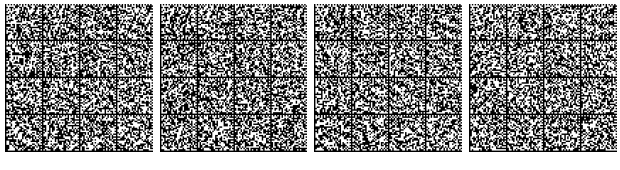
4-*ter*. L'atto amministrativo di cui al comma 2-*bis* e i suoi aggiornamenti sono trasmessi, entro dieci giorni dall'adozione, al Comitato parlamentare per la sicurezza della Repubblica.

5. Per l'aggiornamento di quanto previsto dai decreti di cui ai commi 2 e 3 si procede secondo le medesime modalità di cui ai commi 2, 3, 4 e 4-*bis* con cadenza almeno biennale.

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.

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

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

*b)* ai fini della verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego, definisce le metodologie di verifica e di test e svolge le attività di cui al comma 6, lettera *a)*, dettando, se del caso, anche prescrizioni di utilizzo al committente; a tali fini il CVCN si avvale anche di laboratori dallo stesso accreditati secondo criteri stabiliti da un decreto del Presidente del Consiglio dei ministri, adottato entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, su proposta del 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;

*c)* elabora e adotta, previo conforme avviso del Tavolo interministeriale di cui all'articolo 6 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, schemi di certificazione cibernetica, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea, laddove, per ragioni di sicurezza nazionale, gli schemi di certificazione esistenti non siano ritenuti adeguati alle esigenze di tutela del perimetro di sicurezza nazionale cibernetica.

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

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

*b)* assolvono l'obbligo di notifica di cui al comma 3, lettera *a)*, che costituisce anche adempimento, rispettivamente, dell'obbligo di notifica di cui agli articoli 12 e 14 del decreto legislativo 18 maggio 2018, n. 65, e dell'analogo obbligo previsto ai sensi dell'articolo 16-*ter* del codice di cui al decreto legislativo 1° agosto 2003, n. 259, e delle correlate

disposizioni attuative; a tal fine, oltre a quanto previsto dal comma 3, lettera *a)*, anche in relazione alle disposizioni di cui all'articolo 16-*ter* del codice di cui al decreto legislativo 1° agosto 2003, n. 259, il CSIRT Italia inoltra le notifiche ricevute ai sensi del predetto comma 3, lettera *a)*, autorità nazionale competente NIS di cui all'articolo 7 del decreto legislativo 18 maggio 2018, n. 65.

9. Salvo che il fatto costituisca reato:

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

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

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

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

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

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

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

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

10. L'impiego di prodotti e di servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera *b)*, in assenza della comunicazione o del superamento dei test o in violazione delle condizioni di cui al comma 6, lettera *a)*, comporta, oltre alle sanzioni di cui al comma 9, lettere *d)* ed *e)*, l'applicazione della sanzione amministrativa accessoria della incapacità ad assumere incarichi di direzione, amministrazione e controllo nelle persone giuridiche e nelle imprese, per un periodo di tre anni a decorrere dalla data di accertamento della violazione.

11. Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera *b)*, o al comma 6, lettera *a)*, o delle attività ispettive e di vigilanza previste dal comma 6, lettera *c)*, fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera *b)*, o ai fini delle comunicazioni di cui al comma 6, lettera *a)*, o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera *c)* od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni.

11-*bis*. All'articolo 24-*bis*, comma 3, del decreto legislativo 8 giugno 2001, n. 231, dopo le parole: «di altro ente pubblico,» sono inserite le seguenti: «e dei delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105,».

12. Le autorità competenti per l'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative sono la Presidenza del Consiglio dei ministri, per i soggetti pubblici e per i soggetti di cui all'articolo 29 del codice 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.

13. Ai fini dell'accertamento e dell'irrogazione delle sanzioni amministrative di cui al comma 9, si osservano le disposizioni contenute nel capo I, sezioni I e II, della legge 24 novembre 1981, n. 689.

14. Per i dipendenti dei soggetti pubblici di cui al comma 2-*bis*, la violazione delle disposizioni di cui al presente articolo può costituire causa di responsabilità disciplinare e amministrativo-contabile.

15. Le autorità titolari delle attribuzioni di cui al presente decreto assicurano gli opportuni raccordi con il Dipartimento delle informazioni per la sicurezza e con l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, quale autorità di contrasto nell'esercizio delle attività di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

16. La Presidenza del Consiglio dei ministri, per lo svolgimento delle funzioni di cui al presente decreto può avvalersi dell'Agenzia per l'Italia Digitale (AgID) sulla base di apposite convenzioni, nell'ambito delle risorse finanziarie e umane disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica.

17. Al decreto legislativo 18 maggio 2018, n. 65, sono apportate le seguenti modificazioni:

*a)* all'articolo 4, comma 5, dopo il primo periodo è aggiunto il seguente:

«Il Ministero dello sviluppo economico inoltra tale elenco al punto di contatto unico e all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.»;

*b)* all'articolo 9, comma 3, le parole «e il punto di contatto unico» sono sostituite dalle seguenti:

«, il punto di contatto unico e l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155,».

18. Gli eventuali adeguamenti alle prescrizioni di sicurezza definite ai sensi del presente articolo, delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici di cui al comma 2-*bis*, sono effettuati con le risorse finanziarie disponibili a legislazione vigente.

19. Per la realizzazione, l'allestimento e il funzionamento del CVCN di cui ai commi 6 e 7 è autorizzata la spesa di euro 3.200.000 per l'anno 2019 e di euro 2.850.000 per ciascuno degli anni dal 2020 al 2023 e di euro 750.000 annui a decorrere dall'anno 2024. Per la realizzazione, l'allestimento e il funzionamento del Centro di valutazione del Ministero dell'interno, di cui ai commi 6 e 7, è autorizzata la spesa di euro 200.000 per l'anno 2019 e di euro 1.500.000 per ciascuno degli anni 2020 e 2021.

19-*bis*. Il Presidente del Consiglio dei ministri coordina la coerente attuazione delle disposizioni del presente decreto che disciplinano il perimetro di sicurezza nazionale cibernetica, anche avvalendosi del Dipartimento delle informazioni per la sicurezza, che assicura gli opportuni raccordi con le autorità titolari delle attribuzioni di cui al presente decreto e con i soggetti di cui al comma 1 del presente articolo. Entro sessanta giorni dalla data di entrata in vigore del regolamento di cui al comma 6, il Presidente del Consiglio dei ministri trasmette alle Camere una relazione sulle attività svolte.

19-*ter*. Nei casi in cui sui decreti del Presidente del Consiglio dei ministri previsti dal presente articolo è acquisito, ai fini della loro adozione, il parere del Consiglio di Stato, i termini ordinatori stabiliti dal presente articolo sono sospesi per un periodo di quarantacinque giorni.».

— La Direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, concernente il trattamento delle acque reflue urbane, è pubblicata nella G.U.C.E. 30 maggio 1991, n. L 135.

— La Direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008 relativa ai rifiuti e che abroga alcune direttive è pubblicata nella G.U.U.E. 22 novembre 2008, n. L 312.

— Si riportano gli articoli 3, comma 1, lettere *g)* e *i)*, e 18 del decreto legislativo 18 maggio 2018, n. 65 (Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione):

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

*a) - f)* (*omissis*);

*g)* operatore di servizi essenziali, soggetto pubblico o privato, della tipologia di cui all'allegato II, che soddisfa i criteri di cui all'articolo 4, comma 2;

*h)* (*omissis*);

*i)* fornitore di servizio digitale, qualsiasi persona giuridica che fornisce un servizio digitale;

l)- *aa)* (*Omissis*).».

«Art. 18 *(Notifica volontaria)*. — 1. I soggetti che non sono stati identificati come operatori di servizi essenziali e non sono fornitori di servizi digitali possono notificare, su base volontaria, gli incidenti aventi un impatto rilevante sulla continuità dei servizi da loro prestati.

2. Nel trattamento delle notifiche, il CSIRT Italia applica la procedura di cui all'articolo 12.

3. Le notifiche obbligatorie sono trattate prioritariamente rispetto alle notifiche volontarie.

4. Le notifiche volontarie sono trattate soltanto qualora tale trattamento non costituisca un onere sproporzionato o eccessivo.

5. La notifica volontaria non può avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica.».

— Si riporta l'articolo 17 del 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), convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, come modificato dalla presente legge:

«Art. 17 *(Disposizioni transitorie e finali)*. — 1. Per lo svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, di cui all'articolo 7, l'Agenzia può provvedere, oltre che con proprio personale, con l'ausilio dell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

2. Per lo svolgimento delle funzioni relative all'attuazione e al controllo dell'esecuzione dei provvedimenti assunti da parte del Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro, l'Agenzia provvede con l'ausilio dell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

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

*4. Il personale dell'Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni, riveste la qualifica di pubblico ufficiale. La trasmissione immediata delle notifiche di incidente ricevute dal CSIRT Italia all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis *del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, costituisce adempimento dell'obbligo di cui all'articolo 331 del codice di procedura penale*.

4-*bis*. Fermo restando quanto previsto dal comma 4, l'Agenzia trasmette al procuratore nazionale antimafia e antiterrorismo i dati, le notizie e le informazioni rilevanti per l'esercizio delle funzioni di cui all'articolo 371-*bis* del codice di procedura penale.

*4-*bis*.1. Nei casi in cui l'Agenzia ha notizia di un attacco ai danni di uno dei sistemi informatici o telematici di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale e in ogni caso quando risulti interessato taluno dei soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge perimetro, all'articolo 3, comma 1, lettere* g) *e* i)*, del decreto legislativo NIS ovvero all'articolo 40, comma 3, alinea, del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259, fermo restando quanto previsto dal comma 4 del presente articolo, procede alle attività di cui all'articolo 7, comma 1, lettere* n) *e n-*bis*), e ne informa senza ritardo il procuratore nazionale antimafia e antiterrorismo, ai sensi del comma 4-*bis *del presente articolo.*

*4-*bis*.2. Fuori dei casi di cui al comma 4-*bis*.1, quando acquisisce la notizia dei delitti di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale, il pubblico ministero ne dà tempestiva informazione all'Agenzia e assicura, altresì, il raccordo informativo con l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione ai fini di cui all'articolo 7-*bis *del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.*

*4-*bis*.3. In ogni caso, il pubblico ministero impartisce le disposizioni necessarie ad assicurare che gli accertamenti urgenti siano compiuti tenendo conto delle attività svolte dall'Agenzia, a fini di resilienza, di cui all'articolo 7, comma 1, lettere* n) *e n-*bis*), e può disporre il differimento di una o più delle predette attività, con provvedimento motivato adottato senza ritardo, per evitare un grave pregiudizio per il corso delle indagini.*

*4-*bis*.4. Il pubblico ministero, quando procede ad accertamenti tecnici irripetibili in relazione ai delitti di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale, informa senza ritardo l'Agenzia, che mediante propri rappresentanti può assistere al conferimento dell'incarico e partecipare agli accertamenti. Le disposizioni del primo periodo si applicano anche quando agli accertamenti si procede nelle forme dell'incidente probatorio.*

4-*ter*. Al fine di consentire la piena operatività dell'Agenzia, le disposizioni di cui all'articolo 15, commi 1 e 2, del decreto-legge 24 aprile 2014, n. 66, convertito, con modificazioni, dalla legge 23 giugno 2014, n. 89, non si applicano alle autovetture utilizzate dall'Agenzia per i servizi istituzionali di tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico.

4-quater. *La disciplina del procedimento sanzionatorio amministrativo dell'Agenzia è definita con regolamento che stabilisce, in particolare, termini e modalità per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia ai sensi del presente decreto e delle altre disposizioni che assegnano poteri accertativi e sanzionatori all'Agenzia. Il regolamento di cui al primo periodo è adottato, entro novanta giorni dalla data di entrata in vigore della presente disposizione, con decreto del Presidente del Consiglio dei ministri, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, sentito il Comitato interministeriale per la cybersicurezza e acquisito il parere delle competenti Commissioni parlamentari. Fino alla data di entrata in vigore del regolamento di cui al presente comma, ai procedimenti sanzionatori si applicano, per ciascuna fase procedimentale di cui al primo periodo, le disposizioni contenute nelle sezioni I e II del capo I della legge 24 novembre 1981, n. 689.*

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

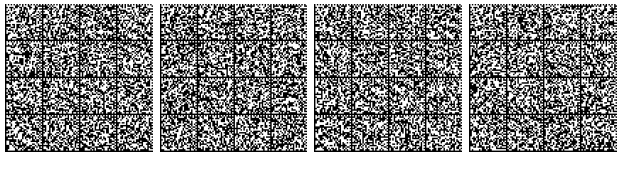
*a)* per assicurare la prima operatività dell'Agenzia, mediante l'individuazione di appositi spazi, in via transitoria e per un massimo di ventiquattro mesi, secondo opportune intese con le amministrazioni interessate, per l'attuazione delle disposizioni del presente decreto;

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

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

6. In relazione al trasferimento delle funzioni di cui all'articolo 7, comma 1, lettera *m)*, dall'AgID all'Agenzia, i decreti di cui al





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

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

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

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

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

8.1. Ai fini di cui al comma 8, l'Agenzia si avvale altresì, sino al 31 dicembre 2023, di un contingente di personale, nel limite di cinquanta unità, appartenente alle pubbliche amministrazioni, alle autorità indipendenti e alle società a controllo pubblico, messo a disposizione dell'Agenzia stessa su specifica richiesta e secondo modalità individuate d'intesa con i soggetti pubblici e privati di appartenenza. I relativi oneri sono a carico dell'Agenzia e ai fini del trattamento retributivo si applicano le disposizioni del regolamento di cui all'articolo 12, comma 1. Il personale di cui al primo periodo, fatta eccezione per il personale proveniente dalle società a controllo pubblico, può essere inquadrato, con provvedimento dell'Agenzia adottato ai sensi dell'articolo 5, comma 3, del regolamento di cui al decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223, nel ruolo del personale di cui all'articolo 12, comma 2, lettera *a)*, non oltre il termine indicato al medesimo primo periodo del presente comma. Al relativo inquadramento si provvede, mediante apposite selezioni, con le modalità e le procedure definite con provvedimento dell'Agenzia, adottato ai sensi del medesimo articolo 5, comma 3, del regolamento di cui al decreto del Presidente del Consiglio dei ministri n. 223 del 2021, sulla base di criteri di valorizzazione delle pregresse esperienze e anzianità di servizio, delle competenze acquisite, dei requisiti di professionalità posseduti e dell'impiego nell'Agenzia. Al personale inquadrato ai sensi dei periodi terzo e quarto del presente comma si applicano le disposizioni del regolamento di cui all'articolo 12, comma 1, anche in materia di opzione per il trattamento previdenziale. Il personale di cui al comma 8, lettera *b)*, già inserito nel ruolo del personale dell'Agenzia, può essere reinquadrato secondo i medesimi criteri di cui al quarto periodo del presente comma con provvedimento dell'Agenzia adottato, ai sensi del citato articolo 5, comma 3, del regolamento di cui al decreto del Presidente del Consiglio dei ministri n. 223 del 2021, entro il 31 dicembre 2023, senza effetti retroattivi. Il personale di cui al terzo periodo del presente comma è computato nel numero dei posti previsti per la prima operatività dell'Agenzia, di cui all'articolo 12, comma 4.

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

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

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

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

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

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

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

— Si riportano gli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124 (Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto):

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

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

3. Il DIS svolge i seguenti compiti:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Il Presidente del Consiglio dei ministri, con proprio decreto, nomina e revoca il direttore dell'AISE, scelto tra dirigenti di prima fascia o equiparati dell'amministrazione dello Stato, sentito il CISR. L'incarico ha la durata massima di otto anni ed è conferibile, senza soluzione di continuità, anche con provvedimenti successivi, ciascuno dei quali di durata non superiore al quadriennio.

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

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

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

«Art. 7 *(Agenzia informazioni e sicurezza interna)*. — 1. È istituita l'Agenzia informazioni e sicurezza interna (AISI), alla quale è affidato il compito di ricercare ed elaborare nei settori di competenza tutte le informazioni utili a difendere, anche in attuazione di accordi internazionali, la sicurezza interna della Repubblica e le

istituzioni democratiche poste dalla Costituzione a suo fondamento da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica.

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

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

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

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

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

7. Il Presidente del Consiglio dei ministri nomina e revoca, con proprio decreto, il direttore dell'AISI, scelto tra i dirigenti di prima fascia o equiparati dell'amministrazione dello Stato, sentito il CISR. L'incarico ha la durata massima di otto anni ed è conferibile, senza soluzione di continuità, anche con provvedimenti successivi, ciascuno dei quali di durata non superiore al quadriennio.

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

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

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

*Note all'art. 2:*

— Per l'articolo 1, comma 2-*bis*, del citato decreto-legge 21settembre 2019, n.105, si veda nelle note all'articolo 1.

— Per l'articolo 3, comma 1, lettere *g)* e *i)*, del citato decreto legislativo 18 maggio 2018, n. 65, si veda nelle note all'articolo 1.

— Si riporta l'articolo 40, comma 3, del decreto legislativo 1°agosto 2003, n. 259 (Codice delle comunicazioni elettroniche):

«Art. 40 *(Sicurezza delle reti e dei servizi)*. — 1. - 2. (*omissis*).

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

*a)* adottano le misure individuate dall'Agenzia di cui al comma 1, lettera *a)*;

*b)* comunicano all'Agenzia e al Computer Security Incident Response Team (CSIRT), istituito ai sensi dell'articolo 8 del decreto legislativo 18 maggio 2018, n. 65, ogni significativo incidente di sicurezza secondo quanto previsto dal comma 1, lettera *b)*.

4. - 8. (*omissis*).».

*Note all'art. 3:*

— Per l'articolo 1, comma 3-*bis*, del citato decreto-legge 21settembre 2019, n.105, si veda nelle note all'articolo 1.

*Note all'art. 4:*

— Si riporta l'articolo 7 del citato decreto-legge 14 giugno 2021, n. 82, come modificato dalla presente legge:

«Art. 7 *(Funzioni dell'Agenzia per la cybersicurezza nazionale)*. — 1. L'Agenzia:

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

*b)* predispone la strategia nazionale di cybersicurezza;

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

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

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

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

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

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

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

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

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

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

*h)* assume tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera *c)*, del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione

delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri n. 131 del 2020;

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

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

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

*m*-bis*) provvede, anche attraverso un'apposita sezione nell'ambito della strategia di cui alla lettera* b)*, allo sviluppo e alla diffusione di standard, linee guida e raccomandazioni al fine di rafforzare la cybersicurezza dei sistemi informatici, alla valutazione della sicurezza dei sistemi crittografici nonché all'organizzazione e alla gestione di attività di divulgazione finalizzate a promuovere l'utilizzo della crittografia, anche a vantaggio della tecnologia blockchain, come strumento di cybersicurezza. L'Agenzia, anche per il rafforzamento dell'autonomia industriale e tecnologica dell'Italia, promuove altresì la collaborazione con centri universitari e di ricerca per la valorizzazione dello sviluppo di nuovi algoritmi proprietari, la ricerca e il conseguimento di nuove capacità crittografiche nazionali nonché la collaborazione internazionale con gli organismi esteri che svolgono analoghe funzioni. A tale fine, è istituito presso l'Agenzia, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, il Centro nazionale di crittografia, il cui funzionamento è disciplinato con provvedimento del direttore generale dell'Agenzia stessa. Il Centro nazionale di crittografia svolge le funzioni di centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato, ferme restando le competenze dell'Ufficio centrale per la segretezza, di cui all'articolo 9 della legge 3 agosto 2007, n. 124, con riferimento alle informazioni e alle attività previste dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera* l)*, della citata legge n. 124 del 2007, nonché le competenze degli organismi di cui agli articoli 4, 6 e 7 della medesima legge*;

m-*ter*) provvede alla qualificazione dei servizi cloud per la pubblica amministrazione nel rispetto della disciplina dell'Unione europea e del regolamento di cui all'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221;

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

n-*bis*) nell'ambito delle funzioni di cui al primo periodo della lettera *n)*, svolge ogni attività diretta all'analisi e al supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi, con la collaborazione dei soggetti pubblici o privati che hanno subìto incidenti di sicurezza informatica o attacchi informatici. La mancata collaborazione di cui al primo periodo è valutata ai fini dell'applicazione delle sanzioni previste dall'articolo 1, commi 10 e 14, del decreto-legge perimetro, per i soggetti di cui all'articolo 1, comma 2-*bis*, del medesimo decreto-legge perimetro, di cui all'articolo 3, comma 1, lettere *g)* e *i)*, del decreto legislativo NIS e di cui all'articolo 40, comma 3, alinea, del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259; restano esclusi gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, nonché gli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124;

*n*-ter*) provvede alla raccolta, all'elaborazione e alla classificazione dei dati relativi alle notifiche di incidenti ricevute dai soggetti che a ciò siano tenuti in osservanza delle disposizioni vigenti. Tali dati sono resi pubblici nell'ambito della relazione prevista dall'articolo 14, comma 1, quali dati ufficiali di riferimento degli attacchi informatici portati ai soggetti che operano nei settori rilevanti per gli interessi nazionali nel campo della cybersicurezza. Agli adempimenti previsti dalla presente lettera si provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente;*

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

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

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

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

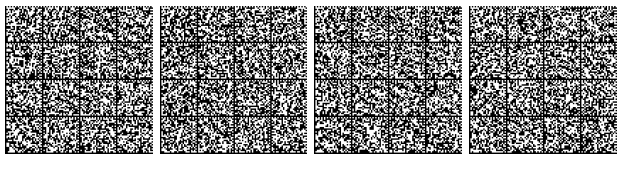
*s)* stipula accordi bilaterali e multilaterali, anche mediante il coinvolgimento del settore privato e industriale, con istituzioni, enti e organismi di altri Paesi per la partecipazione dell'Italia a programmi di cybersicurezza, assicurando il necessario raccordo con le altre amministrazioni a cui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

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

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

*v)* promuove la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza, in particolare favorendo l'attivazione di percorsi formativi univer-





sitari in materia, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati; nello svolgimento di tali compiti, l'Agenzia può avvalersi anche delle strutture formative e delle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri interessati;

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

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

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

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

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

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

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

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

*Note all'art. 5:*

— Si riporta l'articolo 8 del citato decreto-legge 14 giugno 2021, n. 82 come modificato dalla presente legge:

«Art. 8 *(Nucleo per la cybersicurezza).* — 1. Presso l'Agenzia è costituito, in via permanente, il Nucleo per la cybersicurezza, a supporto del Presidente del Consiglio dei ministri nella materia della cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

2. Il Nucleo per la cybersicurezza è presieduto dal direttore generale dell'Agenzia o, per sua delega, dal vice direttore generale ed è composto dal Consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del DIS, dell'Agenzia informazioni e sicurezza esterna (AISE), di cui all'articolo 6 della legge 3 agosto 2007, n. 124, dell'Agenzia informazioni e sicurezza interna (AISI), di cui all'articolo 7 della legge n. 124 del 2007, di ciascuno dei Ministeri rappresentati nel CIC e del Dipartimento della protezione civile della Presidenza del Consiglio dei ministri. Per gli aspetti relativi alla trattazione di informazioni classificate il Nucleo è integrato da un rappresentante dell'Ufficio centrale per la segretezza di cui all'articolo 9 della legge n. 124 del 2007.

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

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

*4.1. In relazione a specifiche questioni di particolare rilevanza concernenti i compiti di cui all'articolo 9, comma 1, lettera* a)*, il Nucleo può essere convocato nella composizione di cui al comma 4 del presente articolo, di volta in volta estesa alla partecipazione di un rappresentante della Direzione nazionale antimafia e antiterrorismo, della Banca d'Italia o di uno o più operatori di cui all'articolo 1, comma 2*-bis*, del decreto-legge perimetro, nonché di eventuali altri soggetti, interessati alle stesse questioni. Le amministrazioni e i soggetti convocati partecipano alle suddette riunioni a livello di vertice.*

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

*Note all'art. 6:*

— Per gli articoli 6 e 7 della citata legge 3 agosto 2007, n. 124, si veda nelle note all'articolo 1.

— Per l'articolo 7 del citato decreto-legge 14 giugno 2021, n. 82, si veda nelle note all'articolo 4.

— Si riporta l'articolo 3 della citata legge 3 agosto 2007, n. 124:

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

1-*bis*. L'Autorità delegata non può esercitare funzioni di governo ulteriori rispetto a quelle ad essa delegate dal Presidente del Consiglio dei Ministri a norma della presente legge e in materia di cybersicurezza, ad eccezione delle funzioni attribuite al Sottosegretario di Stato alla Presidenza del Consiglio dei ministri, con funzioni di Segretario del Consiglio medesimo.

2.

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

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

— Per l'articolo 17, commi 4 e 4-*bis*, del citato decreto-legge 14 giugno 2021, n.82, si veda nelle note all'articolo 1.».

*Note all'art. 7:*

— Si riporta l'articolo 5 della citata legge 3 agosto 2007, n. 124, come modificato dalla presente legge:

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

2. Il Comitato elabora gli indirizzi generali e gli obiettivi fondamentali da perseguire nel quadro della politica dell'informazione per la

sicurezza, delibera sulla ripartizione delle risorse finanziarie tra il DIS e i servizi di informazione per la sicurezza e sui relativi bilanci preventivi e consuntivi.

3. Il Comitato è presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri *e della cooperazione internazionale*, dal Ministro dell'interno, dal Ministro della difesa, dal Ministro della giustizia, dal Ministro dell'economia e delle finanze, dal Ministro *delle imprese e del made in Italy, dal Ministro dell'ambiente e della sicurezza energetica, dal Ministro dell'agricoltura, della sovranità alimentare e delle foreste, dal Ministro delle infrastrutture e dei trasporti e dal Ministro dell'università e della ricerca*.

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

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

*Note all'art. 8:*

— Si riporta l'articolo 53 del decreto legislativo 30 marzo 2001, n. 165 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche):

«Art. 53 *(Incompatibilità, cumulo di impieghi e incarichi)*. — 1. Resta ferma per tutti i dipendenti pubblici la disciplina delle incompatibilità dettata dagli articoli 60 e seguenti del testo unico approvato con decreto del Presidente della Repubblica 10 gennaio 1957, n. 3, salva la deroga prevista dall'articolo 23-*bis* del presente decreto, nonché, per i rapporti di lavoro a tempo parziale, dall'articolo 6, comma 2, del decreto del Presidente del Consiglio dei ministri 17 marzo 1989, n. 117 e dall'articolo 1, commi 57 e seguenti della legge 23 dicembre 1996, n. 662. Restano ferme altresì le disposizioni di cui agli articoli 267, comma 1, 273, 274, 508 nonché 676 del decreto legislativo 16 aprile 1994, n. 297, all'articolo 9, commi 1 e 2, della legge 23 dicembre 1992, n. 498, all'articolo 4, comma 7, della legge 30 dicembre 1991, n. 412, ed ogni altra successiva modificazione ed integrazione della relativa disciplina.

1-*bis*. Non possono essere conferiti incarichi di direzione di strutture deputate alla gestione del personale a soggetti che rivestano o abbiano rivestito negli ultimi due anni cariche in partiti politici o in organizzazioni sindacali o che abbiano avuto negli ultimi due anni rapporti continuativi di collaborazione o di consulenza con le predette organizzazioni.

2. Le pubbliche amministrazioni non possono conferire ai dipendenti incarichi, non compresi nei compiti e doveri di ufficio, che non siano espressamente previsti o disciplinati da legge o altre fonti normative, o che non siano espressamente autorizzati.

3. Ai fini previsti dal comma 2, con appositi regolamenti, da emanarsi ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, sono individuati gli incarichi consentiti e quelli vietati ai magistrati ordinari, amministrativi, contabili e militari, nonché agli avvocati e procuratori dello Stato, sentiti, per le diverse magistrature, i rispettivi istituti.

3-*bis*. Ai fini previsti dal comma 2, con appositi regolamenti emanati su proposta del Ministro per la pubblica amministrazione e la semplificazione, di concerto con i Ministri interessati, ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, e successive modificazioni, sono individuati, secondo criteri differenziati in rapporto alle diverse qualifiche e ruoli professionali, gli incarichi vietati ai dipendenti delle amministrazioni pubbliche di cui all'articolo 1, comma 2.

4. Nel caso in cui i regolamenti di cui al comma 3 non siano emanati, l'attribuzione degli incarichi è consentita nei soli casi espressamente previsti dalla legge o da altre fonti normative.

5. In ogni caso, il conferimento operato direttamente dall'amministrazione, nonché l'autorizzazione all'esercizio di incarichi che provengano da amministrazione pubblica diversa da quella di appartenenza, ovvero da società o persone fisiche, che svolgano attività d'impresa o commerciale, sono disposti dai rispettivi organi competenti secondo criteri oggettivi e predeterminati, che tengano conto della specifica professionalità, tali da escludere casi di incompatibilità, sia di diritto che di fatto, nell'interesse del buon andamento della pubblica amministrazione o situazioni di conflitto, anche potenziale, di interessi, che pregiudichino l'esercizio imparziale delle funzioni attribuite al dipendente.

6. I commi da 7 a 13 del presente articolo si applicano ai dipendenti delle amministrazioni pubbliche di cui all'articolo 1, comma 2, compresi quelli di cui all'articolo 3, con esclusione dei dipendenti con rapporto di lavoro a tempo parziale con prestazione lavorativa non superiore al cinquanta per cento di quella a tempo pieno, dei docenti universitari a tempo definito e delle altre categorie di dipendenti pubblici ai quali è consentito da disposizioni speciali lo svolgimento di attività libero-professionali. Sono nulli tutti gli atti e provvedimenti comunque denominati, regolamentari e amministrativi, adottati dalle amministrazioni di appartenenza in contrasto con il presente comma. Gli incarichi retribuiti, di cui ai commi seguenti, sono tutti gli incarichi, anche occasionali, non compresi nei compiti e doveri di ufficio, per i quali è previsto, sotto qualsiasi forma, un compenso. Sono esclusi i compensi e le prestazioni derivanti:

*a)* dalla collaborazione a giornali, riviste, enciclopedie e simili;

*b)* dalla utilizzazione economica da parte dell'autore o inventore di opere dell'ingegno e di invenzioni industriali;

*c)* dalla partecipazione a convegni e seminari;

*d)* da incarichi per i quali è corrisposto solo il rimborso delle spese documentate;

*e)* da incarichi per lo svolgimento dei quali il dipendente è posto in posizione di aspettativa, di comando o di fuori ruolo;

*f)* da incarichi conferiti dalle organizzazioni sindacali a dipendenti presso le stesse distaccati o in aspettativa non retribuita;

f-*bis*) da attività di formazione diretta ai dipendenti della pubblica amministrazione nonché di docenza e di ricerca scientifica.

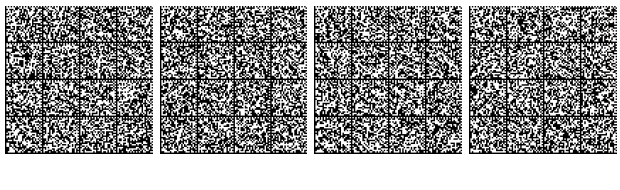
7. I dipendenti pubblici non possono svolgere incarichi retribuiti che non siano stati conferiti o previamente autorizzati dall'amministrazione di appartenenza. Ai fini dell'autorizzazione, l'amministrazione verifica l'insussistenza di situazioni, anche potenziali, di conflitto di interessi. Con riferimento ai professori universitari a tempo pieno, gli statuti o i regolamenti degli atenei disciplinano i criteri e le procedure per il rilascio dell'autorizzazione nei casi previsti dal presente decreto. In caso di inosservanza del divieto, salve le più gravi sanzioni e ferma restando la responsabilità disciplinare, il compenso dovuto per le prestazioni eventualmente svolte deve essere versato, a cura dell'erogante o, in difetto, del percettore, nel conto dell'entrata del bilancio dell'amministrazione di appartenenza del dipendente per essere destinato ad incremento del fondo di produttività o di fondi equivalenti.

7-*bis*. L'omissione del versamento del compenso da parte del dipendente pubblico indebito percettore costituisce ipotesi di responsabilità erariale soggetta alla giurisdizione della Corte dei conti.

8. Le pubbliche amministrazioni non possono conferire incarichi retribuiti a dipendenti di altre amministrazioni pubbliche senza la previa autorizzazione dell'amministrazione di appartenenza dei dipendenti stessi. Salve le più gravi sanzioni, il conferimento dei predetti incarichi, senza la previa autorizzazione, costituisce in ogni caso infrazione disciplinare per il funzionario responsabile del procedimento; il relativo provvedimento è nullo di diritto. In tal caso l'importo previsto come corrispettivo dell'incarico, ove gravi su fondi in disponibilità dell'amministrazione conferente, è trasferito all'amministrazione di appartenenza del dipendente ad incremento del fondo di produttività o di fondi equivalenti.

9. Gli enti pubblici economici e i soggetti privati non possono conferire incarichi retribuiti a dipendenti pubblici senza la previa autorizzazione dell'amministrazione di appartenenza dei dipendenti stessi. Ai fini dell'autorizzazione, l'amministrazione verifica l'insussistenza di situazioni, anche potenziali, di conflitto di interessi. In caso di inosservanza si applica la disposizione dell'articolo 6, comma 1, del decreto legge 28 marzo 1997, n. 79, convertito, con modificazioni, dalla legge 28 maggio 1997, n. 140, e successive modificazioni ed integrazioni. All'accertamento delle violazioni e all'irrogazione delle sanzioni provvede il Ministero delle finanze, avvalendosi della Guardia di finanza,





secondo le disposizioni della legge 24 novembre 1981, n. 689, e successive modificazioni ed integrazioni. Le somme riscosse sono acquisite alle entrate del Ministero delle finanze.

10. L'autorizzazione, di cui ai commi precedenti, deve essere richiesta all'amministrazione di appartenenza del dipendente dai soggetti pubblici o privati, che intendono conferire l'incarico; può, altresì, essere richiesta dal dipendente interessato. L'amministrazione di appartenenza deve pronunciarsi sulla richiesta di autorizzazione entro trenta giorni dalla ricezione della richiesta stessa. Per il personale che presta comunque servizio presso amministrazioni pubbliche diverse da quelle di appartenenza, l'autorizzazione è subordinata all'intesa tra le due amministrazioni. In tal caso il termine per provvedere è per l'amministrazione di appartenenza di 45 giorni e si prescinde dall'intesa se l'amministrazione presso la quale il dipendente presta servizio non si pronunzia entro 10 giorni dalla ricezione della richiesta di intesa da parte dell'amministrazione di appartenenza. Decorso il termine per provvedere, l'autorizzazione, se richiesta per incarichi da conferirsi da amministrazioni pubbliche, si intende accordata; in ogni altro caso, si intende definitivamente negata.

11. Entro quindici giorni dall'erogazione del compenso per gli incarichi di cui al comma 6, i soggetti pubblici o privati comunicano all'amministrazione di appartenenza l'ammontare dei compensi erogati ai dipendenti pubblici.

12. Le amministrazioni pubbliche che conferiscono o autorizzano incarichi, anche a titolo gratuito, ai propri dipendenti comunicano in via telematica, nel termine di quindici giorni, al Dipartimento della funzione pubblica gli incarichi conferiti o autorizzati ai dipendenti stessi, con l'indicazione dell'oggetto dell'incarico e del compenso lordo, ove previsto.

13. Le amministrazioni di appartenenza sono tenute a comunicare tempestivamente al Dipartimento della funzione pubblica, in via telematica, per ciascuno dei propri dipendenti e distintamente per ogni incarico conferito o autorizzato, i compensi da esse erogati o della cui erogazione abbiano avuto comunicazione dai soggetti di cui al comma 11.

14. Al fine della verifica dell'applicazione delle norme di cui all'articolo 1, commi 123 e 127, della legge 23 dicembre 1996, n. 662, e successive modificazioni e integrazioni, le amministrazioni pubbliche sono tenute a comunicare al Dipartimento della funzione pubblica, in via telematica , tempestivamente e comunque nei termini previsti dal decreto legislativo 14 marzo 2013, n. 33, i dati di cui agli articoli 15 e 18 del medesimo decreto legislativo n. 33 del 2013, relativi a tutti gli incarichi conferiti o autorizzati a qualsiasi titolo. Le amministrazioni rendono noti, mediante inserimento nelle proprie banche dati accessibili al pubblico per via telematica, gli elenchi dei propri consulenti indicando l'oggetto, la durata e il compenso dell'incarico nonché l'attestazione dell'avvenuta verifica dell'insussistenza di situazioni, anche potenziali, di conflitto di interessi. Le informazioni relative a consulenze e incarichi comunicate dalle amministrazioni al Dipartimento della funzione pubblica, nonché le informazioni pubblicate dalle stesse nelle proprie banche dati accessibili al pubblico per via telematica ai sensi del presente articolo, sono trasmesse e pubblicate in tabelle riassuntive rese liberamente scaricabili in un formato digitale standard aperto che consenta di analizzare e rielaborare, anche a fini statistici, i dati informatici. Entro il 31 dicembre di ciascun anno il Dipartimento della funzione pubblica trasmette alla Corte dei conti l'elenco delle amministrazioni che hanno omesso di trasmettere e pubblicare, in tutto o in parte, le informazioni di cui al terzo periodo del presente comma in formato digitale standard aperto. Entro il 31 dicembre di ciascun anno il Dipartimento della funzione pubblica trasmette alla Corte dei conti l'elenco delle amministrazioni che hanno omesso di effettuare la comunicazione, avente ad oggetto l'elenco dei collaboratori esterni e dei soggetti cui sono stati affidati incarichi di consulenza.

15. Le amministrazioni che omettono gli adempimenti di cui ai commi da 11 a 14 non possono conferire nuovi incarichi fino a quando non adempiono. I soggetti di cui al comma 9 che omettono le comunicazioni di cui al comma 11 incorrono nella sanzione di cui allo stesso comma 9.

16. Il Dipartimento della funzione pubblica, entro il 31 dicembre di ciascun anno, riferisce al Parlamento sui dati raccolti, adotta le relative misure di pubblicità e trasparenza e formula proposte per il contenimento della spesa per gli incarichi e per la razionalizzazione dei criteri di attribuzione degli incarichi stessi.

16-*bis*. La Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica può disporre verifiche del rispetto delle disposizioni del presente articolo e dell'articolo 1, commi 56 e seguenti, della legge 23 dicembre 1996, n. 662, per il tramite dell'Ispettorato per la funzione pubblica. A tale fine quest'ultimo opera d'intesa con i Servizi ispettivi di finanza pubblica del Dipartimento della Ragioneria generale dello Stato.

16-*ter*. I dipendenti che, negli ultimi tre anni di servizio, hanno esercitato poteri autoritativi o negoziali per conto delle pubbliche amministrazioni di cui all'articolo 1, comma 2, non possono svolgere, nei tre anni successivi alla cessazione del rapporto di pubblico impiego, attività lavorativa o professionale presso i soggetti privati destinatari dell'attività della pubblica amministrazione svolta attraverso i medesimi poteri. I contratti conclusi e gli incarichi conferiti in violazione di quanto previsto dal presente comma sono nulli ed è fatto divieto ai soggetti privati che li hanno conclusi o conferiti di contrattare con le pubbliche amministrazioni per i successivi tre anni con obbligo di restituzione dei compensi eventualmente percepiti e accertati ad essi riferiti.».

— Si riporta l'articolo 17 del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale):

«Art. 17 *(Responsabile per la transizione digitale e difensore civico digitale)*. — 1. Le pubbliche amministrazioni garantiscono l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo in coerenza con le Linee guida. A tal fine, ciascuna pubblica amministrazione affida a un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità. Al suddetto ufficio sono inoltre attribuiti i compiti relativi a:

*a)* coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;

*b)* indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;

*c)* indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;

*d)* accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;

*e)* analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;

*f)* cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera *e)*;

*g)* indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;

*h)* progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;

*i)* promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;

*j)* pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma

elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-*bis*;

j-*bis*) pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera *b)*.

1-*bis*. Per lo svolgimento dei compiti di cui al comma 1, le Agenzie, le Forze armate, compresa l'Arma dei carabinieri e il Corpo delle capitanerie di porto, nonché i Corpi di polizia hanno facoltà di individuare propri uffici senza incrementare il numero complessivo di quelli già previsti nei rispettivi assetti organizzativi.

1-*ter*. Il responsabile dell'ufficio di cui al comma 1 è dotato di adeguate competenze tecnologiche, di informatica giuridica e manageriali e risponde, con riferimento ai compiti relativi alla transizione, alla modalità digitale direttamente all'organo di vertice politico.

1-*quater*. È istituito presso l'AgID l'ufficio del difensore civico per il digitale, a cui è preposto un soggetto in possesso di adeguati requisiti di terzietà, autonomia e imparzialità. Chiunque può presentare al difensore civico per il digitale, attraverso apposita area presente sul sito istituzionale dell'AgID, segnalazioni relative a presunte violazioni del presente Codice e di ogni altra norma in materia di digitalizzazione ed innovazione della pubblica amministrazione da parte dei soggetti di cui all'articolo 2, comma 2. Il difensore civico, accertata la non manifesta infondatezza della segnalazione, la trasmette al Direttore generale dell'AgID per l'esercizio dei poteri di cui all'articolo 18-*bis*.

1-*quinquies*. AgID pubblica sul proprio sito una guida di riepilogo dei diritti di cittadinanza digitali previsti dal presente Codice.

1-*sexies*. Nel rispetto della propria autonomia organizzativa, le pubbliche amministrazioni diverse dalle amministrazioni dello Stato individuano l'ufficio per il digitale di cui al comma 1 tra quelli di livello dirigenziale oppure, ove ne siano privi, individuano un responsabile per il digitale tra le proprie posizioni apicali. In assenza del vertice politico, il responsabile dell'ufficio per il digitale di cui al comma 1 risponde direttamente a quello amministrativo dell'ente.

1-*septies*. I soggetti di cui al comma 1-*sexies* possono esercitare le funzioni di cui al medesimo comma anche in forma associata. È fatta salva la facoltà di avvalersi, mediante apposite convenzioni e senza nuovi o maggiori oneri a carico della finanza pubblica, del supporto di società in house.».

— Per l'articolo 1, comma 2-*bis*, del citato decreto-legge 21 settembre 2019, n.105, si veda nelle note all'articolo 1.

— Per gli articoli 4, 6 e 7 della citata legge 3 agosto 2007, n.124, si veda nelle note all'articolo 1.

*Note all'art. 9:*

— Per l'articolo 1, comma 2-*bis*, del citato decreto-legge 21settembre 2019, n.105, si veda nelle note all'articolo 1.

— Per il citato decreto legislativo 18 maggio 2018, n. 65, si veda nelle note all'articolo 1.

*Note all'art. 10:*

— Per l'articolo 7, comma 1, del citato decreto-legge 14 giugno 2021, n. 82, si veda nelle note all'articolo 4.

*Note all'art. 11:*

— Per l'articolo 17 del citato decreto-legge 14 giugno 2021, n.82, si veda nelle note all'articolo 1.

*Note all'art. 12:*

— Si riporta l'articolo 12 del citato decreto-legge 14 giugno 2021, n. 82, come modificato dalla presente legge:

«Art. 12 *(Personale)*. — 1. Con apposito regolamento è dettata, nel rispetto dei principi generali dell'ordinamento giuridico, anche in deroga alle vigenti disposizioni di legge, ivi incluso il decreto legislativo 30 marzo 2001, n. 165, e nel rispetto dei criteri di cui al presente decreto, la disciplina del contingente di personale addetto all'Agenzia, tenuto conto delle funzioni volte alla tutela della sicurezza nazionale nello spazio cibernetico attribuite all'Agenzia. Il regolamento definisce l'ordinamento e il reclutamento del personale, e il relativo trattamento economico e previdenziale, prevedendo, in particolare, per il personale dell'Agenzia di cui al comma 2, lettera *a)*, un trattamento economico pari a quello in godimento da parte dei dipendenti della Banca d'Italia, sulla scorta della equiparabilità delle funzioni svolte e del livello di responsabilità rivestito. La predetta equiparazione, con riferimento sia al trattamento economico in servizio che al trattamento previdenziale, produce effetti avendo riguardo alle anzianità di servizio maturate a seguito dell'inquadramento nei ruoli dell'Agenzia.

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

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

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

*c)* la possibilità di avvalersi di un contingente di esperti, non superiore a cinquanta unità, composto da personale, collocato fuori ruolo o in posizione di comando o altra analoga posizione prevista dagli ordinamenti di appartenenza, proveniente da pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, con esclusione del personale docente, educativo, amministrativo, tecnico e ausiliario delle istituzioni scolastiche, ovvero da personale non appartenente alla pubblica amministrazione, in possesso di specifica ed elevata competenza in materia di cybersicurezza e di tecnologie digitali innovative, nello sviluppo e gestione di processi complessi di trasformazione tecnologica e delle correlate iniziative di comunicazione e disseminazione, nonché di significativa esperienza in progetti di trasformazione digitale, ivi compreso lo sviluppo di programmi e piattaforme digitali con diffusione su larga scala. Il regolamento, a tali fini, disciplina la composizione del contingente e il compenso spettante per ciascuna professionalità;

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

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

*f)* le ipotesi di incompatibilità;

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

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

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

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

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

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

3-*bis*. Nell'ambito delle assunzioni a tempo indeterminato attraverso modalità concorsuali, l'Agenzia può riservare una quota non superiore al 50 per cento dei posti messi a concorso per l'assunzione di

personale non dirigenziale in favore dei titolari di rapporto di lavoro a tempo determinato di cui al comma 2, lettera *b)*, nonché del personale proveniente dalle società a controllo pubblico ai sensi dell'articolo 17, comma 8.1, in possesso dei requisiti necessari per l'inquadramento nel ruolo del personale dell'Agenzia di cui al comma 2, lettera *a)*, e che, alla data di pubblicazione del bando, abbiano prestato servizio continuativo per almeno due anni presso la medesima Agenzia.

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

5. Fermo restando l'adeguamento della dotazione organica di livello dirigenziale generale e non generale di cui all'articolo 6, comma 1-*bis*, e le relative decorrenze, la rimanente dotazione organica è progressivamente rideterminata, in linea con il processo di crescita della capacità operativa dell'Agenzia, con decreti del Presidente del Consiglio dei ministri di concerto con il Ministro dell'economia e delle finanze, nei limiti delle risorse finanziarie destinate al personale di cui all'articolo 18, comma 1. Dei provvedimenti adottati in materia di dotazione organica è data tempestiva e motivata comunicazione alle Commissioni parlamentari competenti e al COPASIR.

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

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

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

8-*bis*. In relazione alle assunzioni a tempo determinato di cui al comma 2, lettera *b)*, i relativi contratti per lo svolgimento delle funzioni volte alla tutela della sicurezza nazionale nello spazio cibernetico attribuite all'Agenzia possono prevedere una durata massima di quattro anni, rinnovabile per periodi non superiori ad ulteriori complessivi quattro anni. Delle assunzioni e dei rinnovi disposti ai sensi del presente comma è data comunicazione al COPASIR nell'ambito della relazione di cui all'articolo 14, comma 2.

*8*-ter. *I dipendenti appartenenti al ruolo del personale dell'Agenzia di cui al comma 2, lettera* a)*, che abbiano partecipato, nell'interesse e a spese dell'Agenzia, a specifici percorsi formativi di specializzazione, per la durata di due anni a decorrere dalla data di completamento dell'ultimo dei predetti percorsi formativi non possono essere assunti né assumere incarichi presso soggetti privati al fine di svolgere mansioni in materia di cybersicurezza. I contratti stipulati in violazione di quanto disposto dal presente comma sono nulli. Le disposizioni del presente comma non si applicano al personale cessato dal servizio presso l'Agenzia secondo quanto previsto dalle disposizioni del regolamento adottato ai sensi del presente articolo relative al collocamento a riposo d'ufficio, al raggiungimento del requisito anagrafico previsto dalla legge per la pensione di vecchiaia, alla cessazione a domanda per inabilità o alla dispensa dal servizio per motivi di salute. I percorsi formativi di specializzazione di cui al presente comma sono individuati con determinazione del direttore generale dell'Agenzia, tenendo conto della particolare qualità dell'offerta formativa, dei costi, della durata e del livello di specializzazione che consegue alla frequenza dei suddetti percorsi.*».

*Note all'art. 13:*

— Il decreto-legge 15 marzo 2012, n. 21, recante: «Norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni» e convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, è pubblicato nella *G.U.* 15 marzo 2012, n. 63.

— Si riportano gli articoli 21 e 43 della citata legge 3 agosto 2007, n. 124:

«Art. 21 *(Contingente speciale del personale)*. — 1. Con apposito regolamento è determinato il contingente speciale del personale addetto al DIS e ai servizi di informazione per la sicurezza, istituito presso la Presidenza del Consiglio dei ministri.

Il regolamento disciplina altresì, anche in deroga alle vigenti disposizioni di legge e nel rispetto dei criteri di cui alla presente legge, l'ordinamento e il reclutamento del personale garantendone l'unitarietà della gestione, il relativo trattamento economico e previdenziale, nonché il regime di pubblicità del regolamento stesso.

2. Il regolamento determina, in particolare:

*a)* l'istituzione di un ruolo unico del personale dei servizi di informazione per la sicurezza e del DIS, prevedendo le distinzioni per le funzioni amministrative, operative e tecniche;

*b)* la definizione di adeguate modalità concorsuali e selettive, aperte anche a cittadini esterni alla pubblica amministrazione, per la scelta del personale;

*c)* i limiti temporali per le assunzioni a tempo determinato nel rispetto della normativa vigente per coloro che, ai sensi della lettera *e)*, non vengono assunti tramite concorso;

*d)* l'individuazione di una quota di personale chiamato a svolgere funzioni di diretta collaborazione con il direttore generale del DIS e con i direttori dei servizi di informazione per la sicurezza, la cui permanenza presso i rispettivi organismi è legata alla permanenza in carica dei medesimi direttori;

*e)* il divieto di assunzione diretta, salvo casi di alta e particolare specializzazione debitamente documentata, per attività assolutamente necessarie all'operatività del DIS e dei servizi di informazione per la sicurezza;

*f)* le ipotesi di incompatibilità, collegate alla presenza di rapporti di parentela entro il terzo grado o di affinità entro il secondo grado o di convivenza o di comprovata cointeressenza economica con dipendenti dei servizi di informazione per la sicurezza o del DIS, salvo che l'assunzione avvenga per concorso; qualora il rapporto di parentela o di affinità o di convivenza o di cointeressenza economica riguardi il direttore generale del DIS o i direttori dei servizi di informazione per la sicurezza, l'incompatibilità è assoluta;

*g)* il divieto di affidare incarichi a tempo indeterminato a chi è cessato per qualunque ragione dal rapporto di dipendenza dal DIS e dai servizi di informazione per la sicurezza;

*h)* i criteri per la progressione di carriera;

*i)* la determinazione per il DIS e per ciascun servizio della percentuale minima dei dipendenti del ruolo di cui alla lettera *a)*;

*l)* i casi eccezionali di conferimento di incarichi ad esperti esterni, nei limiti e in relazione a particolari profili professionali, competenze o specializzazioni;

*m)* i criteri e le modalità relativi al trattamento giuridico ed economico del personale che rientra nell'amministrazione di provenienza al fine del riconoscimento delle professionalità acquisite e degli avanzamenti di carriera conseguiti;

*n)* i criteri e le modalità per il trasferimento del personale del ruolo di cui alla lettera *a)* ad altra amministrazione.

3. Per il reclutamento del personale addetto al DIS e ai servizi di informazione per la sicurezza non si applicano le norme di cui alla legge 12 marzo 1999, n. 68, e successive modificazioni, e all'articolo 16 della legge 28 febbraio 1987, n. 56, e successive modificazioni.

4. Le assunzioni effettuate in violazione dei divieti previsti dalla presente legge o dal regolamento sono nulle, ferma restando la responsabilità personale, patrimoniale e disciplinare di chi le ha disposte.

5. Il regolamento definisce la consistenza numerica, le condizioni e le modalità del passaggio del personale della Segreteria generale del CESIS, del SISMI e del SISDE nel ruolo di cui al comma 2, lettera *a)*.

6. Il regolamento definisce, nei limiti delle risorse finanziarie previste a legislazione vigente e fermo restando quanto stabilito dal comma 6 dell'articolo 29 della presente legge, il trattamento economico onnicomprensivo del personale appartenente al DIS, all'AI-

SE e all'AISI, costituito dallo stipendio, dall'indennità integrativa speciale, dagli assegni familiari e da una indennità di funzione, da attribuire in relazione al grado, alla qualifica e al profilo rivestiti e alle funzioni svolte.

7. È vietato qualsiasi trattamento economico accessorio diverso da quelli previsti dal regolamento. In caso di rientro nell'amministrazione di appartenenza o di trasferimento presso altra pubblica amministrazione, è escluso il mantenimento del trattamento economico principale e accessorio maturato alle dipendenze dei servizi di informazione per la sicurezza, fatte salve le misure eventualmente disposte ai sensi della lettera *m)* del comma 2.

8. Il regolamento disciplina i casi di cessazione dei rapporti di dipendenza, di ruolo o non di ruolo.

9. Il regolamento stabilisce le incompatibilità preclusive del rapporto con il DIS e con i servizi di informazione per la sicurezza, in relazione a determinate condizioni personali, a incarichi ricoperti e ad attività svolte, prevedendo specifici obblighi di dichiarazione e, in caso di violazione, le conseguenti sanzioni.

10. Non possono svolgere attività, in qualsiasi forma, alle dipendenze del Sistema di informazione per la sicurezza persone che, per comportamenti o azioni eversive nei confronti delle istituzioni democratiche, non diano sicuro affidamento di scrupolosa fedeltà alla Costituzione.

11. In nessun caso il DIS e i servizi di informazione per la sicurezza possono, nemmeno saltuariamente, avere alle loro dipendenze o impiegare in qualità di collaboratori o di consulenti membri del Parlamento europeo, del Parlamento o del Governo nazionali, consiglieri regionali, provinciali, comunali o membri delle rispettive giunte, dipendenti degli organi costituzionali, magistrati, ministri di confessioni religiose e giornalisti professionisti o pubblicisti.

12. Tutto il personale che presta comunque la propria opera alle dipendenze o a favore del DIS o dei servizi di informazione per la sicurezza è tenuto, anche dopo la cessazione di tale attività, al rispetto del segreto su tutto ciò di cui sia venuto a conoscenza nell'esercizio o a causa delle proprie funzioni.».

«Art. 43 *(Procedura per l'adozione dei regolamenti)*. — 1. Salvo che non sia diversamente stabilito, le disposizioni regolamentari previste dalla presente legge sono emanate entro centottanta giorni dalla data della sua entrata in vigore, con uno o più decreti del Presidente del Consiglio dei ministri adottati anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, e successive modificazioni, previo parere del Comitato parlamentare di cui all'articolo 30 e sentito il CISR.

2. I suddetti decreti stabiliscono il regime della loro pubblicità, anche in deroga alle norme vigenti.».

— Si riporta l'articolo 134 del regio decreto 18 giugno 1931, n. 773 (Approvazione del testo unico delle leggi di pubblica sicurezza):

«Art. 134. Senza licenza del prefetto è vietato ad enti o privati di prestare opere di vigilanza o custodia di proprietà mobiliari od immobiliari e di eseguire investigazioni o ricerche o di raccogliere informazioni per conto di privati.

Salvo il disposto dell'art. 11, la licenza non può essere conceduta alle persone che non abbiano la cittadinanza italiana ovvero di uno Stato membro dell'Unione europea o siano incapaci di obbligarsi o abbiano riportato condanna per delitto non colposo.

I cittadini degli Stati membri dell'Unione europea possono conseguire la licenza per prestare opera di vigilanza o custodia di beni mobiliari o immobiliari alle stesse condizioni previste per i cittadini italiani.

Il regolamento di esecuzione individua gli altri soggetti, ivi compreso l'institore, o chiunque eserciti poteri di direzione, amministrazione o gestione anche parziale dell'istituto o delle sue articolazioni, nei confronti dei quali sono accertati l'assenza di condanne per delitto non colposo e gli altri requisiti previsti dall'articolo 11 del presente testo unico, nonché dall'articolo 10 della legge 31 maggio 1965, n. 575.

La licenza non può essere conceduta per operazioni che importano un esercizio di pubbliche funzioni o una menomazione della libertà individuale.».

*Note all'art. 14:*

— Per l'articolo 5 della citata legge 3 agosto 2007, n. 124, si veda nelle note all'articolo 7.

— Si riporta l'articolo 10, comma 1, del citato decreto-legge 14 giugno 2021, n. 82:

«Art. 10 *(Gestione delle crisi che coinvolgono aspetti di cybersicurezza)*. — 1. Nelle situazioni di crisi che coinvolgono aspetti di cybersicurezza, nei casi in cui il Presidente del Consiglio dei ministri convochi il CISR in materia di gestione delle predette situazioni di crisi, alle sedute del Comitato sono chiamati a partecipare il Ministro delegato per l'innovazione tecnologica e la transizione digitale e il direttore generale dell'Agenzia.

2.- 5. (*omissis*).».

— Si riporta l'articolo 2, comma 2, del citato decreto legislativo 7 marzo 2005, n. 82:

«Art. 2 *(Finalità e ambito di applicazione)*. — 1. (*omissis*).

2. Le disposizioni del presente Codice si applicano:

*a)* alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione;

*b)* ai gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;

*c)* alle società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera *p)*, del medesimo decreto che non rientrino nella categoria di cui alla lettera *b)*.

2-*bis*. - 6-*bis*. (*omissis*).».

— Si riportano gli articoli 107, comma 2, e 108, commi 3, 4 e 10, del decreto legislativo 31 marzo 2023, n. 36 (Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici):

«Art. 107 *(Principi generali in materia di selezione)*. — 1. (*omissis*).

2. La stazione appaltante può decidere di non aggiudicare l'appalto all'offerente che ha presentato l'offerta economicamente più vantaggiosa se ha accertato che l'offerta non soddisfa gli obblighi in materia ambientale, sociale e del lavoro stabiliti dalla normativa europea e nazionale, dai contratti collettivi o dalle disposizioni internazionali di diritto del lavoro indicate nell'allegato X alla direttiva 2014/24/UE del Parlamento europeo e del Consiglio del 26 febbraio 2014.

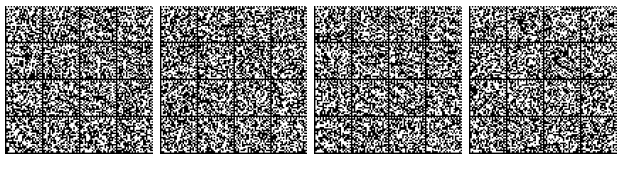
3. (*omissis*).».

«Art. 108 *(Criteri di aggiudicazione degli appalti di lavori, servizi e forniture)*. — 1. – 2. (*omissis*).

3. Può essere utilizzato il criterio del minor prezzo per i servizi e le forniture con caratteristiche standardizzate o le cui condizioni sono definite dal mercato, fatta eccezione per i servizi ad alta intensità di manodopera di cui alla definizione dell'articolo 2, comma 1, lettera *e)*, dell'allegato I.

4. I documenti di gara stabiliscono i criteri di aggiudicazione dell'offerta, pertinenti alla natura, all'oggetto e alle caratteristiche del contratto. In particolare, l'offerta economicamente più vantaggiosa, individuata sulla base del miglior rapporto qualità/prezzo, è valutata sulla base di criteri oggettivi, quali gli aspetti qualitativi, ambientali o sociali, connessi all'oggetto dell'appalto. La stazione appaltante, al fine di assicurare l'effettiva individuazione del miglior rapporto qualità/prezzo, valorizza gli elementi qualitativi dell'offerta e individua criteri tali da garantire un confronto concorrenziale effettivo sui profili tecnici. Nelle attività di approvvigionamento di beni e servizi informatici, le stazioni appaltanti, incluse le centrali di committenza, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del miglior rapporto qualità prezzo per l'aggiudicazione, tengono sempre in considerazione gli elementi di cybersicurezza, attribuendovi specifico e peculiare rilievo nei casi in cui il contesto di impiego è connesso alla tutela degli interessi nazionali strategici. Nei casi di cui al quarto periodo, quando i beni e servizi informatici oggetto di appalto sono impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, la stazione appaltante stabilisce





un tetto massimo per il punteggio economico entro il limite del 10 per cento. Per i contratti ad alta intensità di manodopera, la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del 30 per cento.

5.- 9. (*omissis*).

10. Le stazioni appaltanti possono decidere di non procedere all'aggiudicazione se nessuna offerta risulti conveniente o idonea in relazione all'oggetto del contratto. Tale facoltà è indicata espressamente nel bando di gara o invito nelle procedure senza bando e può essere esercitata non oltre il termine di trenta giorni dalla conclusione delle valutazioni delle offerte.

11. - 12. (*omissis*).».

— Per l'articolo 1 del citato decreto-legge 21settembre 2019, n.105, si veda nelle note all'articolo 1.

*Note all'art. 15:*

— Si riporta l'articolo 16 della legge 21 febbraio 2024, n. 15 (Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2022-2023), come modificato dalla presente legge:

«Art. 16 *(Delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011, e per il recepimento della direttiva (UE) 2022/2556, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario)*. — 1. Il Governo è delegato ad adottare, entro diciotto mesi dalla data di entrata in vigore della presente legge, con le procedure di cui all'articolo 31 della legge 24 dicembre 2012, n. 234, acquisito il parere dell'Agenzia per la cybersicurezza nazionale, uno o più decreti legislativi per l'adeguamento della normativa nazionale al regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, nonché per il recepimento della direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio, del 14 dicembre 2022.

2. Nell'esercizio della delega di cui al comma 1, il Governo è tenuto a seguire, oltre ai princìpi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, anche i seguenti princìpi e criteri direttivi specifici:

*a)* apportare alla normativa vigente, compreso il sistema sanzionatorio, le modifiche e integrazioni necessarie all'adeguamento dell'ordinamento giuridico nazionale al regolamento (UE) 2022/2554 e al recepimento della direttiva (UE) 2022/2556, con l'eventuale esercizio, anche mediante la normativa secondaria di cui alla lettera *d)* del presente comma, delle opzioni previste dal regolamento (UE) 2022/2554. Nell'adozione di tali modifiche e integrazioni il Governo tiene conto degli orientamenti delle autorità di vigilanza europee, degli atti delegati adottati dalla Commissione europea e delle disposizioni legislative nazionali di recepimento delle seguenti direttive strettamente correlate al regolamento (UE) 2022/2554:

1) direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, di cui all'articolo 3 della presente legge;

2) direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, di cui all'articolo 5 della presente legge;

*b)* assicurare che alle autorità competenti, individuate ai sensi dell'articolo 19, paragrafo 1, secondo comma, e dell'articolo 46 del regolamento (UE) 2022/2554, siano attribuiti tutti i poteri di vigilanza, di indagine e sanzionatori per l'attuazione del regolamento (UE) 2022/2554 e della direttiva (UE) 2022/2556, coerentemente con il riparto di competenze nel settore finanziario nazionale;

*c)* attribuire alle autorità di cui alla lettera *b)* del presente comma il potere di imporre le sanzioni e le altre misure amministrative previste dagli articoli 42, paragrafo 6, e 50 del regolamento (UE) 2022/2554, nel rispetto dei limiti edittali e delle procedure previsti dalle disposizioni nazionali che disciplinano l'irrogazione delle sanzioni e l'applicazione delle altre misure amministrative da parte delle autorità anzidette, avuto riguardo al riparto di competenze nel settore finanziario nazionale;

*c*-bis*) apportare alla disciplina applicabile agli intermediari finanziari iscritti nell'albo previsto dall'articolo 106 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, nonché alla società Poste italiane Spa per l'attività del Patrimonio Bancoposta, di cui al regolamento di cui al decreto del Presidente della Repubblica 14 marzo 2001, n. 144, le occorrenti modifiche e integrazioni, anche mediante la normativa secondaria di cui alla lettera* d) *del presente comma, per conseguire un livello elevato di resilienza operativa digitale e assicurare la stabilità del settore finanziario nel suo complesso, in particolare:*

*1) definendo presìdi in materia di resilienza operativa digitale equivalenti a quelli stabiliti nel regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022;*

*2) tenendo conto, nella definizione dei presìdi di cui al numero 1), del principio di proporzionalità e delle attività svolte dagli intermediari finanziari e dal Patrimonio Bancoposta;*

*3) attribuendo alla Banca d'Italia l'esercizio dei poteri di vigilanza, di indagine e sanzionatori di cui alla lettera* b) *nei confronti dei soggetti di cui alla presente lettera*;

*d)* prevedere, ove opportuno, il ricorso alla disciplina secondaria adottata dalle autorità indicate alla lettera *b)* secondo le rispettive competenze.

3. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni competenti provvedono all'adempimento dei compiti derivanti dall'esercizio della delega di cui al presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.».

*Note all'art. 16:*

— Si riporta il testo degli articoli 240, 615-*ter*, 615-*quater*, 617-*bis*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 629, 635-*bis*, 635-*ter*, 635-*quater*, 640, 640-*quater* del codice penale, come modificato dalla presente legge:

«Art. 240 *(Confisca)*. — Nel caso di condanna, il giudice può ordinare la confisca delle cose che servirono o furono destinate a commettere il reato, e delle cose, che ne sono il prodotto o il profitto.

È sempre ordinata la confisca:

1. delle cose che costituiscono il prezzo del reato;

1-*bis*. dei beni e degli strumenti informatici o telematici che risultino essere stati in tutto o in parte utilizzati per la commissione dei reati di cui agli articoli 615-*ter*, 615-*quater*, 615-*quinquies*, 617-*bis*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, 635-*quinquies*, *640, secondo comma, numero 2*-ter*)*, 640-*ter* e 640-*quinquies* nonché dei beni che ne costituiscono il profitto o il prodotto ovvero di somme di denaro, beni o altre utilità di cui il colpevole ha la disponibilità per un valore corrispondente a tale profitto o prodotto, se non è possibile eseguire la confisca del profitto o del prodotto diretti;

2. delle cose, la fabbricazione, l'uso, il porto, la detenzione o l'alienazione delle quali costituisce reato, anche se non è stata pronunciata condanna.

Le disposizioni della prima parte e dei numeri 1 e 1-*bis* del capoverso precedente non si applicano se la cosa o il bene o lo strumento informatico o telematico appartiene a persona estranea al reato. La disposizione del numero 1-*bis* del capoverso precedente si applica anche nel caso di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale.

La disposizione del n. 2 non si applica se la cosa appartiene a persona estranea al reato e la fabbricazione, l'uso, il porto, la detenzione o l'alienazione possono essere consentiti mediante autorizzazione amministrativa.».

«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 due a dieci 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 *minaccia o* 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 *ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare* 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 tre a dieci anni e da quattro a dodici 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 *vantaggio* 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 due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615*-ter*, secondo comma, numero 1).*

*La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615*-ter*, terzo comma.*».

«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 due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615*-ter*, secondo comma, numero 1).*

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.».

«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 quattro a dieci anni* se il fatto è commesso:

*1) in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615*-ter*, terzo comma*;

2) *in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o 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;

*3) (abrogato)*.».

«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.

*Quando ricorre taluna delle circostanze di cui all'articolo 617*-quater*, quarto comma, numero 2), la pena è della reclusione da due a sei anni.*

*Quando ricorre taluna delle circostanze di cui all'articolo 617*-quater*, quarto comma, numero 1), la pena è della reclusione da tre a otto anni.*».

«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 tre a otto 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. 629 *(Estorsione)*. — Chiunque, mediante violenza o minaccia, costringendo taluno a fare o ad omettere qualche cosa, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da cinque a dieci anni e con la multa da euro 1.000 a euro 4.000.

La pena è della reclusione da sette a venti anni e della multa da euro 5.000 a euro 15.000, se concorre taluna delle circostanze indicate *nel terzo comma dell'articolo 628*.

*Chiunque, mediante le condotte di cui agli articoli 615*-ter*, 617*-quater*, 617*-sexies*, 635*-bis*, 635*-quater *e 635*-quinquies *ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità.*»

«Art. 635-*bis (Danneggiamento di informazioni, dati e programmi informatici)*. — Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione *da due a sei anni*.

*La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato.*».

«Art. 635-*ter (Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico)*. — Salvo che il

fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici *di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, è punito con la reclusione da due a sei anni*.

*La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato;*

*3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.*

*La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3).*».

«Art. 635-*quater (Danneggiamento di sistemi informatici o telematici)*. — Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-*bis*, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione *da due a sei anni*.

*La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato.*».

«Art. 640 *(Truffa)*. — Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549:

1. se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare;

2. se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'autorità;

2-*bis*. se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5).

*2-*ter*) se il fatto è commesso a distanza attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione.*

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal *secondo comma, a eccezione di quella di cui al numero 2-*ter*)*.».

«Art. 640-*quater (Applicabilità dell'articolo 322-*ter*)*. — Nei casi di cui agli articoli 640, secondo comma, *numeri 1 e 2-*ter*)*, 640-*bis* e 640-*ter*, secondo comma, con esclusione dell'ipotesi in cui il fatto è commesso con abuso della qualità di operatore del sistema, si osservano, in quanto applicabili, le disposizioni contenute nell'articolo 322-*ter*.».

— Il Capo III-*bis*, Titolo XII, Libro II, come modificato dalla presente legge, reca: «DISPOSIZIONI COMUNI».

*Note all'art. 17:*

— Si riporta il testo degli articoli 51, 406 e 407 del codice di procedura penale, come modificato dalla presente legge:

«Art. 51 *(Uffici del pubblico ministero. Attribuzioni del procuratore della Repubblica distrettuale)*. — 1. Le funzioni di pubblico ministero sono esercitate:

*a)* nelle indagini preliminari e nei procedimenti di primo grado, dai magistrati della procura della Repubblica presso il tribunale;

*b)* nei giudizi di impugnazione dai magistrati della procura generale presso la corte di appello o presso la corte di cassazione.

2. Nei casi di avocazione, le funzioni previste dal comma 1 lettera *a)* sono esercitate dai magistrati della procura generale presso la corte di appello.

Nei casi di avocazione previsti dall'articolo 371-*bis*, sono esercitate dai magistrati della Direzione nazionale antimafia e antiterrorismo.

3. Le funzioni previste dal comma 1 sono attribuite all'ufficio del pubblico ministero presso il giudice competente a norma del capo II del titolo I.

3-*bis*. Quando si tratta dei procedimenti per i delitti, consumati o tentati, di cui agli articoli 416, sesto e settimo comma, 416, realizzato allo scopo di commettere taluno dei delitti di cui agli articoli 12, commi 1, 3 e 3-*ter*, e 12-*bis* del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, 416, realizzato allo scopo di commettere delitti previsti dagli articoli 473 e 474, 517-*quater*,600, 601, 602, 416-*bis*, 416-*ter*, 452-*quaterdecies* e 630 del codice penale, per i 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 previsti dall'articolo 74 del testo unico approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, dall'articolo 291-*quater* del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, le funzioni indicate nel comma 1 lettera *a)* sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente.

3-*ter*. Nei casi previsti dal comma 3-*bis* e dai commi 3-*quater* e 3-*quinquies*, se ne fa richiesta il procuratore distrettuale, il procuratore generale presso la corte di appello può, per giustificati motivi, disporre che le funzioni di pubblico ministero per il dibattimento siano esercitate da un magistrato designato dal procuratore della Repubblica presso il giudice competente.

3-*quater*. Quando si tratta di procedimenti per i delitti consumati o tentati con finalità di terrorismo le funzioni indicate nel comma 1, lettera *a)*, sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente.

3-*quinquies*. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 414-*bis*, 600-*bis*, 600-*ter*, 600-*quater*, 600-*quater*.1, 600-*quinquies*, 609-*undecies*, 615-*ter*, 615-*quater*, 617-*bis*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, *635*-quater.*1, 635*-quinquies*,* 640-*ter* e 640-*quinquies* del codice penale, *o per il delitto di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133,* le funzioni indicate nel comma 1, lettera *a)*, del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente.».

«Art. 406 *(Proroga dei termini)*. — 1. Il pubblico ministero, prima della scadenza, può richiedere al giudice, quando le indagini sono complesse, la proroga del termine previsto dall'articolo 405. La richiesta contiene l'indicazione della notizia di reato e l'esposizione dei motivi che la giustificano.

2. La proroga può essere autorizzata per una sola volta e per un tempo non superiore a sei mesi.

2-*bis*.

2-*ter*.

3. La richiesta di proroga è notificata, a cura del giudice, con l'avviso della facoltà di presentare memorie entro cinque giorni dalla notificazione, alla persona sottoposta alle indagini nonché alla persona offesa dal reato che, nella notizia di reato o successivamente alla sua

presentazione, abbia dichiarato di volere esserne informata. Il giudice provvede entro dieci giorni dalla scadenza del termine per la presentazione delle memorie.

4. Il giudice autorizza la proroga del termine con ordinanza emessa in camera di consiglio senza intervento del pubblico ministero e dei difensori.

5. Qualora ritenga che allo stato degli atti non si debba concedere la proroga, il giudice, entro il termine previsto dal comma 3 secondo periodo, fissa la data dell'udienza in camera di consiglio e ne fa notificare avviso al pubblico ministero, alla persona sottoposta alle indagini nonché, nella ipotesi prevista dal comma 3, alla persona offesa dal reato. Il procedimento si svolge nelle forme previste dall'articolo 127.

5-*bis*. Le disposizioni dei commi 3, 4 e 5 non si applicano se si procede per taluno dei delitti indicati nell'articolo 51 comma 3-*bis* e nell'articolo 407, comma 2, lettera *a)*, *numeri 4), 7*-bis *e 7*-ter*)*. In tali casi, il giudice provvede con ordinanza entro dieci giorni dalla presentazione della richiesta, dandone comunicazione al pubblico ministero.

6. Se non ritiene di respingere la richiesta di proroga, il giudice autorizza con ordinanza il pubblico ministero a proseguire le indagini.

7. Con l'ordinanza che respinge la richiesta di proroga, il giudice, se il termine per le indagini preliminari è già scaduto, fissa un termine non superiore a dieci giorni per la formulazione delle richieste del pubblico ministero a norma dell'articolo 405.

8. Gli atti di indagine compiuti dopo la presentazione della richiesta di proroga e prima della comunicazione del provvedimento del giudice sono comunque utilizzabili sempre che, nel caso di provvedimento negativo, non siano successivi alla data di scadenza del termine originariamente previsto per le indagini.».

«Art. 407 *(Termini di durata massima delle indagini preliminari)*. — 1. Salvo quanto previsto all'articolo 393 comma 4, la durata delle indagini preliminari non può comunque superare diciotto mesi o, se si procede per una contravvenzione, un anno.

2. La durata massima è tuttavia di due anni se le indagini preliminari riguardano:

*a)* i delitti appresso indicati:

1) delitti di cui agli articoli 285, 286, 416-*bis* e 422 del codice penale, 291-*ter*, limitatamente alle ipotesi aggravate previste dalle lettere *a)*, *d)* ed *e)* del comma 2, e 291-*quater*, comma 4, del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43;

2) delitti consumati o tentati di cui agli articoli 575, 628, terzo comma, 629, secondo comma, e 630 dello stesso codice penale;

3) delitti commessi avvalendosi delle condizioni previste dall'articolo 416-*bis* del codice penale ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo;

4) delitti commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale per i quali la legge stabilisce la pena della reclusione non inferiore nel minimo a cinque anni o nel massimo a dieci anni, nonché delitti di cui agli articoli 270, terzo comma e 306, secondo comma, del codice penale;

5) delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo escluse quelle previste dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110;

6) delitti di cui agli articoli 73, limitatamente alle ipotesi aggravate ai sensi dell'articolo 80, comma 2, e 74 del testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza, approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, e successive modificazioni;

7) delitto di cui all'articolo 416 del codice penale nei casi in cui è obbligatorio l'arresto in flagranza;

7-*bis*) dei delitti previsto dagli articoli 600, 600-*bis*, primo comma, 600-*ter*, primo e secondo comma, 601, 602, 609-*bis* nelle ipotesi aggravate previste dall'articolo 609-*ter*, 609-*quater*, 609-*octies* del codice penale, nonché dei delitti previsti dagli articoli 12, comma 3, e 12-*bis* del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286, e successive modificazioni;

*7*-ter*) delitti previsti dagli articoli 615*-ter*, 615*-quater*, 617*-ter*, 617*-quater*, 617*-quinquies*, 617*-sexies*, 635*-bis*, 635*-ter*, 635*-quater*, 635*-quater.*1 e 635*-quinquies *del codice penale, quando il fatto è commesso in danno di 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.*

*b)* notizie di reato che rendono particolarmente complesse le investigazioni per la molteplicità di fatti tra loro collegati ovvero per l'elevato numero di persone sottoposte alle indagini o di persone offese;

*c)* indagini che richiedono il compimento di atti all'estero;

*d)* procedimenti in cui è indispensabile mantenere il collegamento tra più uffici del pubblico ministero a norma dell'articolo 371.

3. Salvo quanto previsto dall'articolo 415- bis, non possono essere utilizzati gli atti di indagine compiuti dopo la scadenza del termine per la conclusione delle indagini preliminari stabilito dalla legge o prorogato dal giudice.

3-*bis*.».

*Note all'art. 18:*

— Si riporta il testo degli articoli 9, 11 e 16-*nonies* del decreto-legge 15 gennaio 1991, n. 8 (Nuove norme in materia di sequestri di persona a scopo di estorsione e per la protezione dei testimoni di giustizia, nonché per la protezione e il trattamento sanzionatorio di coloro che collaborano con la giustizia), convertito, con modificazioni, dalla legge 15 marzo 1991, n. 82, come modificato dalla presente legge:

«Art. 9 *(Condizioni di applicabilità delle speciali misure di protezione)*. — 1. Alle persone che tengono le condotte o che si trovano nelle condizioni previste dai commi 2 e 5 possono essere applicate, secondo le disposizioni del presente Capo, speciali misure di protezione idonee ad assicurarne l'incolumità provvedendo, ove necessario, anche alla loro assistenza.

2. Le speciali misure di protezione sono applicate quando risulta la inadeguatezza delle ordinarie misure di tutela adottabili direttamente dalle autorità di pubblica sicurezza o, se si tratta di persone detenute o internate, dal Ministero della giustizia - Dipartimento dell'amministrazione penitenziaria e risulta altresì che le persone nei cui confronti esse sono proposte versano in grave e attuale pericolo per effetto di talune delle condotte di collaborazione aventi le caratteristiche indicate nel comma 3 e tenute relativamente a delitti commessi per finalità di terrorismo o di eversione dell'ordine costituzionale ovvero ricompresi fra quelli di cui all'articolo 51, comma 3-*bis*, *o all'articolo 371*-bis*, comma 4*-bis*,* del codice di procedura penale e agli articoli 600-*bis*, 600-*ter*, 600-*quater*, anche se relativi al materiale pornografico di cui all'articolo 600-*quater*.1, e 600-*quinquies* del codice penale.

3. Ai fini dell'applicazione delle speciali misure di protezione, assumono rilievo la collaborazione o le dichiarazioni rese nel corso di un procedimento penale. La collaborazione e le dichiarazioni predette devono avere carattere di intrinseca attendibilità. Devono altresì avere carattere di novità o di completezza o per altri elementi devono apparire di notevole importanza per lo sviluppo delle indagini o ai fini del giudizio ovvero per le attività di investigazione sulle connotazioni strutturali, le dotazioni di armi, esplosivi o beni, le articolazioni e i collegamenti interni o internazionali delle organizzazioni criminali di tipo mafioso o terroristico-eversivo o sugli obiettivi, le finalità e le modalità operative di dette organizzazioni.

4. Se le speciali misure di protezione indicate nell'articolo 13, comma 4, non risultano adeguate alla gravità ed attualità del pericolo, esse possono essere applicate anche mediante la definizione di uno speciale programma di protezione i cui contenuti sono indicati nell'articolo 13, comma 5.

5. Le speciali misure di protezione di cui al comma 4 possono essere applicate anche a coloro che convivono stabilmente con le persone indicate nel comma 2 nonché, in presenza di specifiche situazioni, anche a coloro che risultino esposti a grave, attuale e concreto pericolo a causa delle relazioni intrattenute con le medesime persone. Il solo rapporto di parentela, affinità o coniugio, non determina, in difetto di stabile coabitazione, l'applicazione delle misure.

6. Nella determinazione delle situazioni di pericolo si tiene conto, oltre che dello spessore delle condotte di collaborazione o della rilevanza e qualità delle dichiarazioni rese, anche delle caratteristiche di reazione del gruppo criminale in relazione al quale la collaborazione o le dichiarazioni sono rese, valutate con specifico riferimento alla forza di intimidazione di cui il gruppo è localmente in grado di valersi.».

«Art. 11 *(Proposta di ammissione)*. — 1. L'ammissione alle speciali misure di protezione, oltre che i contenuti e la durata di esse, sono di volta in volta deliberati dalla commissione centrale di cui all'articolo 10, comma 2, su proposta formulata dal procuratore della Repubblica il cui ufficio procede o ha proceduto sui fatti indicati nelle dichiarazioni rese dalla persona che si assume sottoposta a grave e attuale pericolo. Allorché sui fatti procede o ha proceduto la Direzione distrettuale antimafia e a essa non è preposto il procuratore distrettuale, ma un suo delegato, la proposta è formulata da quest'ultimo.

2. Quando le dichiarazioni indicate nel comma 1 attengono a procedimenti per taluno dei delitti previsti dall'articolo 51, commi 3-*bis* e 3-*quater*, *o all'articolo 371*-bis*, comma 4*-bis*,* del codice di procedura penale, in relazione ai quali risulta che più uffici del pubblico ministero procedono a indagini collegate a norma dell'articolo 371 dello stesso codice, la proposta è formulata da uno degli uffici procedenti d'intesa con gli altri e comunicata al procuratore nazionale antimafia e antiterrorismo; nel caso di mancata intesa il procuratore nazionale antimafia e antiterrorismo risolve il contrasto.

3. La proposta può essere formulata anche dal Capo della polizia-direttore generale della pubblica sicurezza previa acquisizione del parere del procuratore della Repubblica che, se ne ricorrono le condizioni, è formulato d'intesa con le altre autorità legittimate a norma del comma 2.

4. Quando non ricorrono le ipotesi indicate nel comma 2, l'autorità che formula la proposta può comunque richiedere il parere del procuratore nazionale antimafia e antiterrorismo nonché dei procuratori generali presso le corti di appello interessati allorché ritiene che le notizie, le informazioni e i dati attinenti alla criminalità organizzata di cui il procuratore nazionale antimafia e antiterrorismo o i procuratori generali dispongono per l'esercizio delle loro funzioni, a norma dell'articolo 371-*bis* del codice di procedura penale e del citato articolo 118-*bis* delle relative norme di attuazione, di coordinamento e transitorie, possano essere utili per la deliberazione della commissione centrale.

5. Anche per il tramite del suo presidente, la commissione centrale può esercitare sia la facoltà indicata nel comma 4 sia quella di richiedere il parere del procuratore nazionale antimafia e antiterrorismo o dei procuratori generali presso le corti di appello interessati quando ritiene che la proposta doveva essere formulata dal procuratore della Repubblica d'intesa con altre procure e risulta che ciò non è avvenuto. In tale ultima ipotesi e sempreché ritengano ricorrere le condizioni indicate nel comma 2, il procuratore nazionale antimafia e antiterrorismo e i procuratori generali, oltre a rendere il parere, danno comunicazione dei motivi che hanno originato la richiesta al procuratore generale presso la Corte di cassazione.

6. Nelle ipotesi di cui ai commi 2, 3, 4 e 5, il procuratore nazionale antimafia e antiterrorismo e i procuratori generali presso le corti di appello interessati possono acquisire copie di atti nonché notizie o informazioni dalle autorità giudiziarie che procedono a indagini o a giudizi connessi o collegati alle medesime condotte di collaborazione.

7. La proposta per l'ammissione alle speciali misure di protezione contiene le notizie e gli elementi utili alla valutazione sulla gravità e attualità del pericolo cui le persone indicate nell'articolo 9 sono o possono essere esposte per effetto della scelta di collaborare con la giustizia compiuta da chi ha reso le dichiarazioni. Nella proposta sono elencate le eventuali misure di tutela adottate o fatte adottare e sono evidenziati i motivi per i quali le stesse non appaiono adeguate.

8. Nell'ipotesi prevista dall'articolo 9, comma 3, la proposta del procuratore della Repubblica, ovvero il parere dello stesso procuratore quando la proposta è effettuata dal Capo della polizia - direttore generale della pubblica sicurezza, deve fare riferimento specifico alle caratteristiche del contributo offerto dalle dichiarazioni.».

«Art. 16-*nonies (Benefici penitenziari)*. — 1. Nei confronti delle persone condannate per un delitto commesso per finalità di terrorismo o di eversione dell'ordinamento costituzionale o per uno dei delitti di cui all'articolo 51, comma 3-*bis*, *o all'articolo 371*-bis*, comma 4*-bis*,* del codice di procedura penale, che abbiano prestato, anche dopo la condanna, taluna delle condotte di collaborazione che consentono la concessione delle circostanze attenuanti previste dal codice penale o da disposizioni speciali, la liberazione condizionale, la concessione dei permessi premio e l'ammissione alla misura della detenzione domiciliare prevista dall'articolo 47-*ter* della legge 26 luglio 1975, n. 354, e successive modificazioni, sono disposte su proposta ovvero sentito il procuratore nazionale antimafia e antiterrorismo.

2. Nella proposta o nel parere il procuratore nazionale antimafia e antiterrorismo fornisce ogni utile informazione sulle caratteristiche della collaborazione prestata. Su richiesta del tribunale o del magistrato di sorveglianza, allega alla proposta o al parere copia del verbale illustrativo dei contenuti della collaborazione e, se si tratta di persona sottoposta a speciali misure di protezione, il relativo provvedimento di applicazione.

3. La proposta o il parere indicati nel comma 2 contengono inoltre la valutazione della condotta e della pericolosità sociale del condannato e precisano in specie se questi si è mai rifiutato di sottoporsi a interrogatorio o a esame o ad altro atto di indagine nel corso dei procedimenti penali in cui ha prestato la sua collaborazione. Precisano inoltre gli altri elementi rilevanti ai fini dell'accertamento del ravvedimento anche con riferimento alla attualità dei collegamenti con la criminalità organizzata o eversiva.

4. Acquisiti la proposta o il parere indicati nei commi 2 e 3, il tribunale o il magistrato di sorveglianza, se ritiene che sussistano i presupposti di cui al comma 1, avuto riguardo all'importanza della collaborazione e sempre che sussista il ravvedimento e non vi siano elementi tali da far ritenere la sussistenza di collegamenti con la criminalità organizzata o eversiva, adotta il provvedimento indicato nel comma 1 anche in deroga alle vigenti disposizioni, ivi comprese quelle relative ai limiti di pena di cui all'articolo 176 del codice penale e agli articoli 30-*ter* e 47-*ter* della legge 26 luglio 1975, n. 354, e successive modificazioni. Il provvedimento è specificamente motivato nei casi in cui le autorità indicate nel comma 2 del presente articolo hanno espresso parere sfavorevole. I provvedimenti che derogano ai limiti di pena possono essere adottati soltanto se, entro il termine prescritto dall'articolo 16-*quater* è stato redatto il verbale illustrativo dei contenuti della collaborazione previsto dal medesimo articolo 16-*quater* e, salvo che non si tratti di permesso premio, soltanto dopo la espiazione di almeno un quarto della pena inflitta ovvero, se si tratta di condannato all'ergastolo, dopo l'espiazione di almeno dieci anni di pena.

5. Se la collaborazione prestata dopo la condanna riguarda fatti diversi da quelli per i quali è intervenuta la condanna stessa, i benefici di cui al comma 1 possono essere concessi in deroga alle disposizioni vigenti solo dopo l'emissione della sentenza di primo grado concernente i fatti oggetto della collaborazione che ne confermi i requisiti di cui all'articolo 9, comma 3.

6. Le modalità di attuazione dei provvedimenti indicati nel comma 4 sono stabilite sentiti gli organi che provvedono alla tutela o alla protezione dei soggetti interessati e possono essere tali organi a provvedere alle notifiche, alle comunicazioni e alla esecuzione delle disposizioni del tribunale o del magistrato di sorveglianza.

7. La modifica o la revoca dei provvedimenti è disposta d'ufficio ovvero su proposta o parere delle autorità indicate nel comma 2. Nei casi di urgenza, il magistrato di sorveglianza può disporre con decreto motivato la sospensione cautelativa dei provvedimenti. La sospensione cessa di avere efficacia se, trattandosi di provvedimento di competenza del tribunale di sorveglianza, questo non interviene entro sessanta giorni dalla ricezione degli atti. Ai fini della modifica, della revoca o della sospensione cautelativa dei provvedimenti assumono specifico rilievo quelle condotte tenute dal soggetto interessato che, a norma degli articoli 13-*quater* e 16-*septies*, possono comportare la modifica o la revoca delle speciali misure di protezione ovvero la revisione delle sentenze che hanno concesso taluna delle attenuanti in materia di collaborazione.

8. Quando i provvedimenti di liberazione condizionale, di assegnazione al lavoro all'esterno, di concessione dei permessi premio e di ammissione a taluna delle misure alternative alla detenzione previste dal Titolo I, Capo VI, della legge 26 luglio 1975, n. 354, e successive modificazioni, sono adottati nei confronti di persona sottoposta a speciali misure di protezione, la competenza appartiene al tribunale o al magistrato di sorveglianza del luogo in cui la persona medesima ha eletto il domicilio a norma dell'articolo 12, comma 3-*bis*, del presente decreto».

8-*bis*. Le disposizioni del presente articolo si applicano in quanto compatibili anche nei confronti delle persone condannate per uno dei delitti previsti dal libro II, titolo XII, capo III, sezione I, del codice penale che abbiano prestato, anche dopo la condanna, condotte di collaborazione aventi i requisiti previsti dall'articolo 9, comma 3.».

*Note all'art. 19:*

— Si riporta il testo dell'articolo 13 del decreto-legge 13 maggio 1991, n. 152 (Provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa), convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, come modificato dalla presente legge:

«Art. 13. — 1. In deroga a quanto disposto dall'articolo 267 del codice di procedura penale, l'autorizzazione a disporre le operazioni previste dall'articolo 266 dello stesso codice è data, con decreto motivato, quando l'intercettazione è necessaria per lo svolgimento delle indagini in relazione ad un delitto di criminalità organizzata o di minaccia col mezzo del telefono in ordine ai quali sussistano sufficienti indizi. Nella valutazione dei sufficienti indizi si applica l'articolo 203 del codice di procedura penale. Quando si tratta di intercettazione di comunicazioni tra presenti disposta in un procedimento relativo a un delitto di criminalità organizzata e che avvenga nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione è consentita anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa.

2. Nei casi di cui al comma 1, la durata delle operazioni non può superare i quaranta giorni, ma può essere prorogata dal giudice con decreto motivato per periodi successivi di venti giorni, qualora permangano i presupposti indicati nel comma 1. Nei casi di urgenza, alla proroga provvede direttamente il pubblico ministero; in tal caso si osservano le disposizioni del comma 2 dell'articolo 267 del codice di procedura penale.

3. Negli stessi casi di cui al comma 1 il pubblico ministero e l'ufficiale di polizia giudiziaria possono farsi coadiuvare da agenti di polizia giudiziaria.

*3*-bis*. Le disposizioni dei commi 1, 2 e 3 si applicano anche quando si procede in relazione a taluno dei delitti, consumati o tentati, previsti dall'articolo 371*-bis*, comma 4*-bis*, del codice di procedura penale.».*

*Note all'art. 20:*

— Si riporta il testo dell'articolo 24-*bis* del 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), come modificato dalla presente legge:

«Art. 24-*bis (Delitti informatici e trattamento illecito di dati)*. — 1. In relazione alla commissione dei delitti di cui agli articoli 615-*ter*, 617-*quater*, 617-*quinquies*, 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* del codice penale, si applica all'ente la sanzione pecuniaria *da duecento a settecento quote*.

*1*-bis*. In relazione alla commissione del delitto di cui all'articolo 629, terzo comma, del codice penale, si applica all'ente la sanzione pecuniaria da trecento a ottocento quote.*

2. In relazione alla commissione dei delitti di cui agli articoli 615-*quater* e *635*-quater*.1* del codice penale, si applica all'ente la sanzione pecuniaria *sino a quattrocento quote*.

3. In relazione alla commissione dei delitti di cui agli articoli 491-*bis* e 640-*quinquies* del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, e dei delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.

4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere *a)*, *b)* ed *e)*. *Nei casi di condanna per il delitto indicato nel comma 1*-bis *si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a due anni.* Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere *b)* ed *e)*. Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere *c)*, *d)* ed *e)*.».

*Note all'art. 21:*

— Si riporta il testo dell'articolo 11 della legge 11 gennaio 2018, n. 6 (Disposizioni per la protezione dei testimoni di giustizia), come modificato dalla presente legge:

«Art. 11 *(Proposta di ammissione alle speciali misure di protezione)*. — 1. Nella proposta di ammissione alle speciali misure di protezione l'autorità proponente indica, oltre quanto previsto dall'articolo 13 del decreto-legge 15 gennaio 1991, n. 8, convertito, con modificazioni, dalla legge 15 marzo 1991, n. 82, e dai relativi decreti attuativi, anche la sussistenza dei requisiti stabiliti dall'articolo 2 della presente legge.

2. La proposta di cui al comma 1 del presente articolo è trasmessa alla commissione centrale, che richiede il parere, in caso di delitti di cui all'articolo 51, commi 3-*bis*, 3-*ter* e 3-*quater*, *o all'articolo 371*-bis*, comma 4*-bis*,* del codice di procedura penale, al Procuratore nazionale antimafia e antiterrorismo. La commissione richiede altresì al Servizio centrale di protezione e al prefetto competente per il luogo di dimora di colui che rende le dichiarazioni le informazioni nella loro rispettiva disponibilità, anche con riferimento a quanto previsto dall'articolo 2, comma 1, lettera *e)*, della presente legge.

3. Nel caso in cui la proposta di cui al comma 1 riguardi soggetti di minore età in condizioni di disagio familiare o sociale, essa è altresì trasmessa al tribunale per i minorenni territorialmente competente per l'adozione di eventuali determinazioni di sua competenza.».

*Note all'art. 22:*

— Per l'articolo 17 del citato decreto-legge 14 giugno 2021, n. 82, si veda nelle note all'articolo 1.

*Note all'art. 23:*

— Si riporta il testo dell'articolo 7 della legge 12 agosto 1962, n. 1311 (organizzazione e funzionamento dell'ispettorato generale presso il ministero di grazia e giustizia), come modificato dalla presente legge:

«Art. 7 *(Verifiche ispettive)*. — Il capo dell'Ispettorato generale dispone, in conformità delle direttive impartite dal Ministro, le ispezioni in tutti gli uffici giudiziari allo scopo di accertare se i servizi procedono secondo le leggi, i regolamenti e le istruzioni vigenti. *Nelle ispezioni è verificato altresì il rispetto delle prescrizioni di sicurezza negli accessi alle banche di dati in uso presso gli uffici giudiziari.*

Le ispezioni di cui al comma precedente hanno luogo, di norma, ogni triennio; il capo dell'ispettorato generale può ordinare che esse siano ripetute entro un termine minore negli uffici ove siano state riscontrate o per i quali vengono segnalate deficienze o irregolarità.

Il Ministro può in ogni tempo, quando lo ritenga opportuno, disporre ispezioni negli uffici giudiziari.Il Ministro può altresì disporre ispezioni parziali negli uffici giudiziari, al fine di accertare la produttività *degli stessi,* l'entità e la tempestività del lavoro di singoli magistrati *nonché il rispetto delle prescrizioni di sicurezza negli accessi alle banche di dati in uso presso gli uffici giudiziari»*.

*Note all'art. 24:*

— Si riporta l'articolo 11 del citato decreto-legge 14 giugno 2021, n. 82:

«Art. 11 *(Norme di contabilità e disposizioni finanziarie)*. — 1. Con la legge di bilancio è determinato lo stanziamento annuale da assegnare all'Agenzia da iscrivere sul capitolo di cui all'articolo 18, comma 1, sulla base della determinazione del fabbisogno annuo operata dal Presidente del Consiglio dei ministri, previamente comunicata al COPASIR.

2. Le entrate dell'Agenzia sono costituite da:

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

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

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

*d)* altri proventi patrimoniali e di gestione;

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

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

*g)* ogni altra eventuale entrata.

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

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

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

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

**24G00108**