SENATO DELLA REPUBBLICA

Attesto che il Senato della Repubblica, il 19 giugno 2024, ha approvato il seguente disegno di legge, d'iniziativa del Governo, già approvato dalla Camera dei deputati:

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

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 Parla-

mento 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 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 es-

senziali 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 si-

stemi 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'altera-

zione 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 uffi-

ciale. 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.

IL PRESIDENTE