DISEGNO DI LEGGE

Capo I
Disposizioni in materia di rafforzamento della cybersicurezza nazionale, resilienza delle pubbliche amministrazioni, personale e funzionamento dell'Agenzia per la cybersicurezza nazionale, 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, i comuni con una popolazione superiore ai 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore ai 100.000 abitanti e le aziende sanitarie locali, segnalano e notificano, con le modalità e nei termini di cui al comma 2, 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, aventi impatto su reti, sistemi informativi e servizi informatici. Tra i soggetti di cui al presente comma sono altresì incluse le rispettive società *in house*.
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, un 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 sul sito istituzionale dell'Agenzia per la cybersicurezza nazionale.
3. Nell'ipotesi in cui 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 di cui all'articolo 18, commi 3, 4 e 5, del decreto legislativo 18 maggio 2018, n. 65.
4. 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 comporterà l'applicazione delle disposizioni di cui al comma 5 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 determina del direttore generale dell'Agenzia per la cybersicurezza nazionale, pubblicata nella Gazzetta Ufficiale della Repubblica italiana.
5. Nei casi di reiterata inosservanza dell'obbligo di notifica di cui ai commi 1 e 2, l'Agenzia per la cybersicurezza nazionale applica altresì, nel rispetto delle disposizioni di cui all'articolo 17, comma 4-*quater*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000. La violazione delle disposizioni di cui al comma 1 può costituire causa di responsabilità disciplinare e amministrativo-contabile.
6. Fermi gli obblighi e le sanzioni, anche penali, previsti da altre norme di legge, le disposizioni di cui al presente articolo non si applicano:
a) ai soggetti di cui di cui all'articolo 3, comma 1, lettere g) e i), del decreto legislativo n. 65 del 2018, e a quelli di cui all'articolo 1, comma 2-*bis*, del decreto-legge n. 105 del 2019;
b) agli organi dello Stato preposti alla prevenzione, accertamento e 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, nonché 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 decreto legislativo 1° agosto 2003, n. 259, in presenza di segnalazioni puntuali dell'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità cui essi risultano 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 comporta l'applicazione delle sanzioni di cui all'articolo 1, comma 5, 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 comma 1.

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, il secondo periodo è sostituito dal seguente: «I medesimi soggetti provvedono a effettuare la segnalazione degli incidenti di cui al presente comma senza ritardo, e comunque entro il termine massimo di ventiquattro ore e a effettuare la relativa notifica entro settantadue ore.» e dopo il quarto periodo è aggiunto, in fine, il seguente: «Nei casi di reiterata inosservanza degli obblighi di notifica di cui al presente comma, si applica una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000.».

ART. 4
(*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, 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. 5
(*Disposizioni in materia di coordinamento operativo tra i servizi di informazione per la sicurezza e l'Agenzia per la cybersicurezza nazionale*)

1. Nell'ipotesi in cui i servizi 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-legge14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, i predetti servizi, per il tramite del Dipartimento delle informazioni per la sicurezza, ne informano il Presidente del Consiglio dei ministri o l'Autorità delegata di cui all'articolo 3 della 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 inclusi 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. 6

(*Rafforzamento della resilienza delle pubbliche amministrazioni. Referente per la cybersicurezza*)

1. I soggetti di cui all'articolo 1, comma 1, provvedono a individuare, laddove non 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 procedure di sicurezza delle informazioni;

b) alla produzione e all'aggiornamento di un piano per la gestione del rischio informatico;

c) alla produzione e all'aggiornamento di un documento che definisca ruoli e 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'implementazione 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'implementazione 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 delle qualità professionali possedute. Il predetto referente 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 tal fine, il nominativo del referente per la cybersicurezza è comunicato all'Agenzia per la cybersicurezza nazionale.

3. Le disposizioni di cui al 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, per i quali continuano a trovare applicazione gli obblighi previsti dalle disposizioni di cui alla richiamata disciplina;

b) agli organi dello Stato preposti alla prevenzione, accertamento e 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. 7

(*Funzioni dell'Agenzia per la cybersicurezza nazionale in materia di intelligenza artificiale*)

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 m-*ter*), è inserita la seguente: «m-*quater*) promuove e sviluppa ogni iniziativa, anche di partenariato pubblico-privato, volta a valorizzare l'intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale, anche al fine di favorire un uso etico e corretto dei sistemi basati su tale tecnologia;».

ART. 8

(*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 notifica 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. 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 nel capo I, sezioni I e II, della legge 24 novembre 1981, n. 689.».

ART. 9

(*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, in fine, 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 di cui al presente comma non si applicano al personale cessato dal servizio presso l'Agenzia secondo quanto previsto dalle disposizioni del regolamento adottato in attuazione 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, ovvero alla dispensa dal servizio per motivi di salute. I percorsi formativi di specializzazione di cui al presente comma sono individuati con determina del direttore generale dell'Agenzia, che tenga conto della particolare qualità dell'offerta formativa, dei costi, della durata e del relativo livello di specializzazione che consegue alla frequenza dei suddetti percorsi.».

ART. 10

(Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e misure 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 adottarsi 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 cybersicurezza di cui all'articolo 4 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla 4 agosto 2021, n. 109, sono individuati gli elementi essenziali di cybersicurezza che i soggetti di cui all'articolo 2, comma 2, del 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. Ai fini del presente articolo, per elementi essenziali di cybersicurezza si intende l'insieme di *standard* e regole tecniche la cui conformità 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, incluse le centrali di committenza:

a) possono esercitare la facoltà di cui agli articoli 107, comma 2, e 108, comma 10, del 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 decreto legislativo n. 36 del 2023, inseriscono gli elementi di cybersicurezza di cui al comma 1 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 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.

3. Le disposizioni di cui al comma 1 si applicano anche ai soggetti privati non ricompresi fra quelli di cui all'articolo 2, comma 2, del decreto legislativo 7 marzo 2005, n. 82, e inclusi 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 previsto dall'articolo 1 del decreto-legge n. 105 del 2019, per i casi ivi previsti di 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), del medesimo articolo 1.

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

ART. 11
(*Modifiche al codice penale*)

1. Al codice penale sono apportate le seguenti modificazioni:
   a) 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 le parole: «usa» sono inserite le seguenti: «minaccia o»;

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

2) al terzo comma:

2.1 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»;

2.2 dopo il primo periodo è aggiunto il seguente: «Nei soli casi in cui concorrono anche le circostanze previste dal numero 3) del secondo comma, le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 623-*quater* non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.»;

b) 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 inserito 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, primo periodo.»;

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

d) all'articolo 617-*bis*, dopo il primo comma, è aggiunto 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).»;

e) all'articolo 617-*quater*:

1) al quarto comma:

1.1 le parole «da tre a otto anni» sono sostituite dalle seguenti «da quattro a dieci anni»;

1.2 il numero 1) è sostituito dal seguente: «1) in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615-*ter*, terzo comma, primo periodo;»;

1.3 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»;

1.4 il numero 3) è soppresso;

2) dopo il quarto comma, è aggiunto il seguente: «Le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 623-*quater*, concorrenti con l'aggravante di cui

al quarto comma, numero 1), non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alla predetta aggravante.»;

f) 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 sono aggiunti i seguenti: «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.

Le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 623-*quater*, concorrenti con l'aggravante di cui all'articolo 617-*quater*, quarto comma, numero 1), non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alla predetta aggravante.»;

g) all'articolo 617-*sexies:*

1) al secondo comma, le parole: «da uno a cinque anni» sono sostituite dalle parole: «da tre a otto anni»;

2) dopo il secondo comma, è inserito il seguente: «Le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 623-*quater*, concorrenti con l'aggravante di cui all'articolo 617-*quater*, quarto comma, numero 1), non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alla predetta circostanza aggravante.»;

h) nella rubrica del Capo III-*bis* del Titolo XII, le parole: «sulla procedibilità» sono soppresse;

i) dopo l'articolo 623-*ter* è inserito 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 circostanze dell'azione, ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità.

Le pene previste 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.»;

l) all'articolo 629, 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 nell'ultimo capoverso dell'articolo precedente.»;

m) 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.»;

n) 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 comma 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); in tal caso, le circostanze attenuanti

diverse da quelle di cui agli articoli 89, 98 e 639-*ter* non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.»;

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»;

o) 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.»;

p) 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, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

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, primo periodo.»;

q) 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, 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); in tal caso, le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 639-*ter* non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.»;

r) dopo l'articolo 639-*bis* è inserito 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 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.».

ART. 12

(*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) le parole: «615-*quinquies*» sono soppresse;

2) dopo le parole: «635-*quater*,», sono inserite le parole: «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. 13

(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. 14

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

ART. 15

(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, le parole: «615-*quinquies*» sono sostituite dalle seguenti: «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 aggiunto 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. 16

(Modifiche 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. 17

(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 aggiunti 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 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, di cui all'articolo 3, comma 1, lettere *g*) e *i*), del decreto legislativo 18 maggio 2018, n. 65, ovvero di cui all'articolo 40, comma 3, alinea, del decreto legislativo 1° agosto 2003, n. 259, fermo restando quanto previsto dal comma 4, 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*.»;

4-*bis*.2. Fuori dai 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 si svolgano 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 motivato provvedimento 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 può assistere al conferimento dell'incarico e partecipare agli accertamenti. Le disposizioni di cui al primo periodo si applicano anche quando agli accertamenti si procede nelle forme dell'incidente probatorio.».

ART. 18

(*Disposizioni finanziarie*)

1. Dall'attuazione della presente legge non devono derivare nuovi e maggiori oneri a carico della finanza pubblica. Le amministrazioni pubbliche interessate provvedono all'adempimento delle disposizioni della presente legge con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

2. I proventi delle sanzioni di cui all'articolo 1, comma 5, confluiscono tra le 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.

DISEGNO DI LEGGE RECANTE DISPOSIZIONI IN MATERIA DI RAFFORZAMENTO DELLA CYBERSICUREZZA NAZIONALE E DI REATI INFORMATICI

RELAZIONE

Il **Capo I**, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale, resilienza delle pubbliche amministrazioni, personale e funzionamento dell'Agenzia per la cybersicurezza nazionale, nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici", **agli articoli da 1 a 10** contiene disposizioni riguardanti la cybersicurezza nazionale finalizzate a conseguire una più elevata capacità di protezione e risposta di fronte a emergenze cibernetiche. L'attuale contesto geo-politico, infatti, caratterizzato in particolare dai gravi conflitti internazionale in atto, favorisce l'incremento delle minacce informatiche e richiede, pertanto, in modo sempre più incalzante, il raggiungimento di un alto livello di cybersicurezza, attraverso l'attuazione di efficaci misure di gestione dei relativi rischi, nonché la necessità di un'immediata e quanto più completa conoscenza situazionale.

La proposta normativa risponde alla necessità che si è venuta a profilare sempre di più nell'ultimo periodo di far emergere in modo più puntuale la minaccia informatica diretta ai soggetti dalla PA non ricompresi nel Perimetro di sicurezza nazionale cibernetica (di cui al decreto-legge 21 settembre 2019, n. 105) né al momento interessati dalla direttiva NIS, considerato che potrebbero essere interessati dalla direttiva NIS 2, allo stato in fase di recepimento.

Le disposizioni di cui al Capo I del presente provvedimento, dunque, individuano norme necessarie per sviluppare capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, fermo restando le opzioni che saranno definite riguardo all'ambito soggettivo di applicazione della NIS 2.

L'**articolo 1**, rubricato "Obblighi di notifica di incidenti", richiede alle pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, alle regioni e alle province autonome di Trento e Bolzano, ai comuni con una popolazione superiore ai 100.000 abitanti e, comunque, ai comuni capoluoghi di regione, nonché alle società di trasporto pubblico urbano con bacino di utenza non inferiore ai 100.000 abitanti e alle aziende sanitarie locali, di segnalare e notificare gli incidenti indicati nella tassonomia di cui all'articolo 1, comma 3-bis, del decreto-legge 21 settembre 2019, n. 105, aventi impatto su reti, sistemi informativi e

servizi informatici di pertinenza. Sono tenute alla segnalazione e alla notifica anche le società in house di cui si avvalgono i richiamati soggetti (**comma 1**).

Lo stesso articolo 1 stabilisce le modalità e le tempistiche per effettuare la segnalazione e la notifica che, in termini di impatto e sostenibilità, sono limitate solo ad una tassonomia di incidenti di maggiore entità (**comma 2**). Viene considerata anche l'ipotesi in cui i richiamati soggetti interessati effettuino notifiche volontarie di incidenti al di fuori dei casi indicati nella tassonomia di cui al comma 1, nel qual caso si applicano le disposizioni di cui all'articolo 18, commi da 3 a 5, del decreto legislativo 18 maggio 2018, n. 65 (**comma 3**).

In un'ottica di gradualità, sono, inoltre, disciplinate le conseguenze derivanti dall'inosservanza dell'obbligo di notifica di cui al presente articolo, consistenti, nel caso di prima inosservanza, in una preliminare comunicazione dell'Agenzia per la cybersicurezza nazionale all'interessato, che la reiterazione dell'inosservanza comporterà l'applicazione delle sanzioni indicate nel successivo comma 5, e in forme di vigilanza collaborativa attraverso l'invio da parte della medesima Agenzia di ispezioni volte a sostenere l'amministrazione interessata nello sforzo di rafforzamento della propria postura di resilienza cibernetica, anche al fine di verificare l'attuazione degli interventi di rafforzamento della resilienza loro direttamente indicati dall'Agenzia, ovvero previsti da apposite linee guida adottate dalla stessa. Le modalità di tali ispezioni saranno disciplinate con determina del direttore generale dell'Agenzia, pubblicata nella Gazzetta Ufficiale della Repubblica italiana. Per i casi di reiterata inosservanza dell'obbligo di notifica, l'Agenzia per la cybersicurezza nazionale potrà applicare una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000. La violazione delle disposizioni di cui al comma 1 può costituire causa di responsabilità disciplinare e amministrativo-contabile (**commi 4** e **5**).

Infine, è prevista l'esclusione dall'ambito di applicazione dei richiamati obblighi, fermi gli obblighi e le sanzioni, anche penali, previsti da altre norme di legge, dei soggetti di cui di cui all'articolo 3, comma 1, lettere g) e i), del decreto legislativo n. 65 del 2018 (c.d. soggetti NIS), di quelli di cui all'articolo 1, comma 2-bis, del decreto-legge n. 105 del 2019 (c.d. soggetti Perimetro), nonché degli organi dello Stato preposti alla prevenzione, accertamento e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, e degli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124 (**comma 6**).

L'**articolo 2,** rubricato "Mancato o ritardato adeguamento a segnalazioni dell'Agenzia per la cybersicurezza nazionale", stabilisce un obbligo di adottare gli interventi risolutivi in conseguenza delle segnalazioni che l'Agenzia per la cybersicurezza nazionale effettua circa specifiche vulnerabilità.

Tale obbligo si riferisce ai soggetti indicati nel comma 1 dell'articolo 1 del presente provvedimento, nonché ai soggetti Perimetro, ai soggetti NIS, e ai soggetti di cui

all'articolo 40, comma 3, alinea, del decreto legislativo 1° agosto 2003, n. 259 (c.d. soggetti Telco), e riguarda le segnalazioni effettuate dall'Agenzia relative alle vulnerabilità cui tali soggetti risultano potenzialmente esposti (**comma 1**).

È prevista l'applicazione di sanzioni per la mancata o ritardata adozione dei richiamati interventi, nonché una causa di esclusione dall'applicazione delle stesse sanzioni nel caso in cui motivate esigenze di natura tecnico-organizzativa, tempestivamente comunicate all'Agenzia per la cybersicurezza nazionale, impediscano l'adozione degli interventi opportuni o ne comportino il differimento oltre il termine indicato (**comma 2**).

L'**articolo 3**, rubricato "Norme di raccordo con le disposizioni del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133)", modifica l'articolo 1, comma 3-bis, di tale decreto-legge, per finalità di raccordo e coordinamento con le disposizioni recate dal presente provvedimento. In particolare, si prevede, anche per i soggetti Perimetro, l'applicazione della medesima procedura – che consta delle due distinte fasi della segnalazione e della notifica – nonché degli stessi termini, introdotti dall'articolo 1 del presente provvedimento, in relazione alle ipotesi di notifica già previste per gli stessi soggetti Perimetro dal richiamato comma 3-bis, e cioè in relazione a quegli incidenti aventi impatto su reti, sistemi informativi e servizi informatici, di pertinenza di tali soggetti, diversi da quelli inseriti nel Perimetro. È stata, conseguentemente, prevista l'applicazione delle medesime sanzioni introdotte dall'articolo 1 del presente provvedimento per i casi di reiterata violazione dell'obbligo di notifica. (**comma 1**).

L'**articolo 4**, rubricato "Disposizioni in materia di Nucleo per la cybersicurezza", prevede una specifica modalità di funzionamento del Nucleo per la cybersicurezza di cui all'articolo 8 del decreto-legge 14 giugno 2021, n. 82, in relazione a specifiche questioni di particolare rilevanza concernenti i compiti di proposta di iniziative in materia di cybersicurezza del Paese. In particolare, è prevista la possibile convocazione del Nucleo con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati, 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 n. 105 del 2019, nonché di eventuali altri soggetti, interessati alle stesse questioni.

L'**articolo 5**, rubricato "Disposizioni in materia di coordinamento operativo tra i servizi di informazione per la sicurezza e l'Agenzia per la cybersicurezza nazionale", stabilisce la possibilità di differire le attività di resilienza previste dall'articolo 7, comma 1, lettere n) ed n-bis), del decreto-legge n. 82 del 2021, nei casi in cui i servizi di cui agli articoli 6 e 7 della legge 3 agosto 2007, n. 124, avuta notizia di un evento o un incidente informatici, lo ritengano strettamente necessario per motivi legati al perseguimento delle finalità istituzionali del Sistema di informazione per la sicurezza della Repubblica. Di tale necessità, i predetti servizi, per il tramite del Dipartimento delle informazioni per la sicurezza, ne danno informazione al Presidente del Consiglio dei ministri, oppure,

laddove istituita, all'Autorità delegata di cui all'articolo 3 della medesima legge n. 124 del 2007 (**comma 1**).

Nei richiamati casi, è previsto che 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, possa disporre il differimento degli obblighi informativi cui è in ogni caso tenuta l'Agenzia medesima, ai sensi delle disposizioni vigenti, ivi inclusi 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 (**comma 2**).

L'**articolo 6**, rubricato "Rafforzamento della resilienza delle pubbliche amministrazioni. Referente per la cybersicurezza", reca norme che mirano al rafforzamento della resilienza delle pubbliche amministrazioni, proseguendo, in tal modo, nella realizzazione dell'obiettivo anticipato con la direttiva presidenziale del 6 luglio 2023.

In particolare, l'articolo 6 stabilisce che le pubbliche amministrazioni indicate nell'articolo 1, comma 1, del presente provvedimento, debbano provvedere a individuare, laddove non già presente, una struttura, anche tra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, preposta alle relative attività di cybersicurezza (**comma 1**) e presso la quale opererà la istituenda figura del referente per la cybersicurezza, che svolge, tra l'altro, la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale (**comma 2**).

È, inoltre, prevista l'esclusione dall'ambito di applicazione dei richiamati obblighi dei soggetti di cui all'articolo 1, comma 2-bis, del decreto-legge n. 105 del 2019 (soggetti Perimetro), per i quali continuano a trovare applicazione gli obblighi previsti dalle disposizioni di cui alla richiamata disciplina, nonché degli organi dello Stato preposti alla prevenzione, accertamento e 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 (**comma 3**).

L'**articolo 7**, rubricato "Funzioni dell'Agenzia per la cybersicurezza nazionale in materia di intelligenza artificiale", modifica l'articolo 7, comma 1, del decreto-legge 14 giugno 2021, n. 82, inserendo la lettera m-quater), finalizzata a prevedere, in ragione del ruolo di Autorità nazionale per la cybersicurezza, la possibilità per l'Agenzia di promuovere e sviluppare ogni iniziativa, anche di partenariato pubblico-privato, per la valorizzazione dell'intelligenza artificiale come risorsa per il rafforzamento della sicurezza e della resilienza cibernetiche nazionali, anche al fine di favorire un uso etico e corretto dei sistemi basati su tale tecnologia (**comma 1**).

L'**articolo 8**, rubricato "Procedimento amministrativo sanzionatorio per l'accertamento e la contestazione delle violazioni in materia di cybersicurezza di competenza dell'Agenzia per la cybersicurezza nazionale", modifica l'articolo 17 del decreto-legge 14 giugno

2021, n. 82 prevedendo la possibilità di adottare 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, un regolamento per la disciplina del procedimento sanzionatorio amministrativo dell'Agenzia per la cybersicurezza nazionale che stabilisca, in particolare, termini e modalità per l'accertamento, la contestazione e la notifica delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia ai sensi del citato decreto-legge n. 82 del 2021 e delle altre disposizioni che assegnano poteri accertativi e sanzionatori all'Agenzia. Fino all'entrata in vigore di tale regolamento, da adottarsi entro 90 giorni dalla data di entrata in vigore della presente legge, ai procedimenti sanzionatori si applicano, per ciascuna delle richiamate fasi procedimentali (accertamento, contestazione e notifica delle violazioni della normativa in materia di cybersicurezza e irrogazione delle relative sanzioni), le disposizioni contenute nel capo I, sezioni I e II, della legge 24 novembre 1981, n. 689.

L'**articolo 9**, rubricato "Disposizioni in materia di personale dell'Agenzia per la cybersicurezza nazionale", stabilisce un divieto, della durata di due anni, di assunzione, anche di incarichi, presso soggetti privati finalizzata allo svolgimento di mansioni in materia di cybersicurezza per i dipendenti appartenenti al ruolo del personale dell'Agenzia che abbiano partecipato, nell'interesse e a spese dell'Agenzia, a specifici percorsi formativi di specializzazione. Il medesimo articolo 9 prevede specifiche cause di esclusione dall'applicazione del richiamato divieto nel caso di collocamento a riposo d'ufficio, di raggiungimento del requisito anagrafico previsto dalla legge per la pensione di vecchiaia, di cessazione a domanda per inabilità, ovvero di dispensa dal servizio per motivi di salute. I percorsi formativi di specializzazione che danno luogo al predetto divieto di assunzione, sono individuati con determina del direttore generale dell'Agenzia, che tenga conto della particolare qualità dell'offerta formativa, dei costi, della durata e del relativo livello di specializzazione che consegue alla frequenza dei suddetti percorsi (**comma 1**).

L'**articolo 10**, rubricato "Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e misure di raccordo con il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133", reca disposizioni dirette a indicare criteri di cybersicurezza in tema di appalti pubblici. In particolare, è prevista l'adozione di un decreto del Presidente del Consiglio dei ministri, entro 120 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 cybersicurezza di cui all'articolo 4 del decreto-legge 14 giugno 2021, n. 82, con cui sono individuati gli elementi essenziali di cybersicurezza da tenere in considerazione in relazione alle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici (**comma 1**).

Le disposizioni dettate mirano a promuovere maggiore garanzia delle esigenze di cybersicurezza, nel caso in cui le attività di approvvigionamento siano connesse alla tutela degli interessi nazionali strategici prevedendo un richiamo all'applicazione delle disposizioni del decreto legislativo n. 36 del 2023 "Codice dei contratti pubblici) con specifico riferimento agli articoli 107 e 108 dello stesso (**comma 2**).

Le richiamate disposizioni vengono coordinate con quanto stabilito dal decreto-legge n. 105 del 2019 per i casi ivi previsti di approvvigionamento di prodotti, processi, servizi ICT e associate infrastrutture destinati alle reti, ai sistemi informativi e per l'espletamento dei servizi informatici conferiti nel perimetro di sicurezza nazionale cibernetica (**commi 3 e 4**).

Il **Capo II** reca "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 ricomprende gli articoli da 11 a 18, che vengono di seguito partitamente esaminati.

L'**articolo 11** contiene le modifiche al codice penale.

Si interviene, innanzitutto, sul delitto di **accesso abusivo ad un sistema informatico**, di cui all'articolo 615-*ter* del codice ***(lett. a)***.

Quanto alle aggravanti previste dal secondo comma, sono state raddoppiate le soglie edittali (comminandosi ora la pena della reclusione da due a dieci anni), la circostanza di cui al numero 2) è stata ampliata al fine di affiancare all'uso della violenza anche l'impiego della minaccia, mentre in quella di cui al numero 3) è stata contemplata altresì l'ipotesi in cui dal fatto derivi «*la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare*» dei dati, delle informazioni o dei programmi contenuti nel sistema informativo.

Vengono altresì innalzate le pene previste dal terzo comma per i casi in cui l'oggetto materiale delle condotte delittuose sia costituito da 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. Per l'ipotesi base si prevede la pena della reclusione da tre a dieci anni, mentre per le fattispecie aggravate da quattro a dodici anni. Limitatamente alle circostanze previste dal numero 3) del secondo comma, si introduce un divieto di bilanciamento, stabilendosi che «*le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 623*-quater *non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti*»[1].

Quanto alla fattispecie prodromica di **detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o**

[1] Delle attenuanti introdotte con il nuovo articolo 623-*quater* si dirà a proposito delle modifiche apportate dalle ***lett. h) e i)*** della disposizione in commento.

telematici, prevista dall'articolo 615-*quater* del codice ***(lett. b)***, oltre ad ampliarsi il dolo specifico «di profitto» in quello «di vantaggio», si interviene sul sistema delle aggravanti, che vengono sostanzialmente mantenute, sostituendosi l'improprio rinvio all'articolo 617-*quater*, quarto comma, con il richiamo alle corrispondenti aggravanti di cui all'articolo 615-*ter* e, contestualmente, distribuendole in due successivi commi e irrobustendosi le relative cornici edittali. Al secondo comma si prevede, infatti, la pena della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-*ter*, secondo comma, numero 1), mentre al terzo viene comminata la reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-*ter*, terzo comma, primo periodo.

Anche l'intervento (apparentemente abrogativo) operato sull'ulteriore fattispecie prodromica di **detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico,** di cui all'articolo 615-*quinquies* ***(lett. c)***, risponde innanzitutto ad esigenze di riordino sistematico, giacché la disposizione viene in realtà ricollocata all'articolo 635-*quater*.1 nel più appropriato contesto dei delitti di danneggiamento ***(lett. p)***. Vengono inoltre introdotte anche per tale fattispecie le aggravanti appena illustrate con riferimento all'articolo 615-*quater*.

Analoga estensione, seppur limitata alle sole circostanze di cui all'articolo 615-*ter*, secondo comma, numero 1), viene operata per il delitto di **detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche**, previsto dall'articolo 617-*bis* ***(lett. d)***.

L'intervento operato sull'articolo 617-*quater*, relativo al delitto di **intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche**, ha determinato un innalzamento dei limiti edittali previsti per le aggravanti ed un riallineamento, di natura sistematica, del quarto comma al sistema delle aggravanti previste per l'accesso abusivo a sistema informatico, dal quale è stato altresì "importato" – al nuovo quinto comma – il divieto di bilanciamento ***(lett. e)***.

Per il delitto di **detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche**, di cui all'art. 617-*quinquies*, l'intervento è consistito in un innalzamento dei limiti edittali delle fattispecie aggravate, simile a quello a suo tempo visto per l'articolo 635-*quater*.1 ***(lett. f)***. Il nuovo secondo comma prevede la pena della reclusione da due a sei anni quando ricorra taluna delle circostanze di cui all'articolo 617-*quater*, quarto comma, numero 2), mentre per i casi di cui al numero 1) i commi successivi comminano la reclusione da tre a otto anni e prevedono il divieto di bilanciamento con le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 623-*quater*, nei termini già in precedenza illustrati.

Quanto al **delitto di falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche**, previsto dall'articolo 617-*sexies*, s'è rivista la cornice edittale per le ipotesi aggravate (ora innalzata in una forbice da tre a otto anni) e, al terzo comma, è stato anche introdotto il divieto di bilanciamento di cui sopra ***(lett. g).***

In correlazione con il descritto inasprimento sanzionatorio, è parso in parte necessario, in parte opportuno, prevedere **due circostanze attenuanti** volte a mitigarne gli effetti, introducendo al (rinominato) Capo III-*bis* del Titolo XII ***(lett. h)*** un nuovo articolo 623-*quater* ***(lett. i)***.

Ed invero, al fine di prevenire qualsiasi possibile profilo di frizione dei più severi limiti edittali introdotti con i princìpi costituzionali, si è innanzitutto prevista – al primo comma – una circostanza diminuente correlata alla **lieve entità del fatto**, all'uopo riproducendo i tradizionali indicatori di cui all'articolo 311 c.p. (natura, specie, mezzi, modalità o circostanze dell'azione; particolare tenuità del danno o del pericolo). Con il secondo comma, per stimolare **forme di collaborazione *ab intra***, viene introdotta una diminuente (in questo caso *ad effetto speciale*, con riduzione delle pene dalla metà a due terzi) a favore di colui che «*si adoper[i] 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*». Il terzo comma della disposizione, infine, sempre con la finalità di garantire l'assoluta ortodossia costituzionale dell'intervento, **sottrae entrambe le circostanze al divieto di prevalenza** sulla recidiva reiterata e sulle altre circostanze di cui all'articolo 69, quarto comma.

In ragione della specifica gravità e della frequenza di ricatti realizzati attraverso la minaccia o l'attuazione di "attacchi" informatici, al terzo comma dell'articolo 629 è stata introdotta **un'autonoma figura di estorsione** per i casi in cui essa venga realizzata «*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*», assoggettandola a più severe comminatorie edittali (da sei a dodici anni di reclusione e da 5.000 a 10.000 euro di multa, per l'ipotesi base; da otto a ventidue anni di reclusione e da 6.000 a 18.000 euro di multa, nelle fattispecie aggravate) ***(lett. l)***.

Per il delitto di **danneggiamento di informazioni, dati e programmi informatici,** previsto dall'articolo 635-*bis*, oltre ad aggravarsi il trattamento sanzionatorio sia per l'ipotesi base sia per le fattispecie aggravate (è ora comminata la reclusione da due a sei anni per la prima e da tre a otto anni per le seconde), le originarie circostanze aggravanti connesse all'impiego della violenza o della minaccia, nonché alle qualità personali dell'agente, sono state ampliate attraverso il riallineamento a quelle previste dall'articolo 615-*ter*, secondo comma, numeri 1) e 2) ***(lett. m)***. Identico intervento è stato realizzato per il delitto di **danneggiamento di sistemi informatici o telematici**, previsto dall'articolo 635-*quater* ***(lett. o)***.

Quanto al **danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità**, di cui all'articolo 635-*ter*, oltre a semplificarsene il *nomen juris* (in danneggiamento di informazioni, dati e programmi informatici «*pubblici o di interesse pubblico*»), si è intervenuti al fine di: - uniformare a quella già prevista dall'articolo 615-*ter*, comma 3, l'indicazione della natura delle informazioni, dei dati e dei programmi informatici protetti; - aumentare le soglie edittali per l'ipotesi base e le fattispecie aggravate (reclusione da due a sei anni per la prima, da tre a otto anni per le seconde); - uniformare a quella di cui all'articolo 615-*ter*, comma 2, l'elencazione delle circostanze aggravanti; - comminare la pena della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorra con taluna delle circostanze cui al numero 3), escludendo - in tal caso - che circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 639-*ter* possano essere ritenute equivalenti o prevalenti ***(lett. n)***[2]. Anche in questo caso, un intervento sostanzialmente identico è stato operato sul delitto di **danneggiamento di sistemi informatici o telematici di pubblico utilità** (ora «di pubblico *interesse*»), previsto dall'articolo 635-*quinquies*, del quale si è altresì adeguata la formulazione del primo comma riproducendo estensivamente la descrizione del «*fatto di cui all'articolo 635-quater*» in precedenza impiegata nella norma ***(lett. q)***.

Della (apparente) nuova introduzione dell'articolo 635-*quater*.1, relativo alla fattispecie prodromica di **detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico,** già prevista dall'articolo 615-*quinquies*, s'è già detto nel commentare l'avvenuta abrogazione di tale disposizione ***(lett. p)***.

Un ultimo intervento si è concretizzato, infine, nell'introduzione del nuovo articolo 639-*ter*, con cui sono state previste **due circostanze attenuanti per i casi di lieve entità del fatto e di collaborazione**, del tutto corrispondenti – per struttura, efficacia e regime di bilanciamento – a quelle esaminate in occasione dell'illustrazione dell'articolo 623-*quater*, alla quale può dunque senz'altro operarsi integrale rinvio ***(lett. r)***

Il potenziamento della risposta sanzionatoria illustrata all'articolo 11 è corredato dall'estensione ai reati di criminalità informatica più gravi di alcune delle **disposizioni processuali penali** riservate dal legislatore alle fattispecie di reato di maggiore allarme sociale.

In particolare, **l'articolo 12:**

[2] Come subito si rileverà, all'articolo 639-*ter* sono state introdotte due circostanze attenuanti identiche a quelle già illustrate nel commentare il nuovo articolo 623-*quater*.

- soppresso il riferimento all'articolo 615-*quinquies* (inserito nel nuovo 635.-*quater*.1), **integra** il catalogo dei reati informatici attribuiti dall'articolo **51, comma 3-*quinquies***, alla **competenza del procuratore distrettuale**, includendovi le fattispecie delittuose di cui agli articoli 635.-*quater*.1 (detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico), 635-*quinquies* (danneggiamento di sistemi informatici o telematici di pubblico interesse) del codice penale, nonché 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 (che punisce le false informazioni tese a ostacolare o condizionare la formazione e trasmissione dell'elenco delle reti, sistemi informatici e informativi da parte degli operatori compresi nel perimetro di sicurezza cibernetica, le procedure di affidamento delle forniture di strumenti destinati ai servizi e sistemi informatici, o le attività ispettive o di vigilanza su reti, sistemi informatici e servizi informatici (***lettera a***);
- **estende** ai reati informatici di cui al catalogo previsto al numero 7-*ter* dell'articolo 407, comma 2, lettera a), introdotto alla successiva lettera c), la portata applicativa della deroga disposta all'**articolo 406, comma 5-*bis***, così escludendo la richiamata categoria di reati dal regime ordinario di notifica dell'avviso della richiesta di **proroga delle indagini preliminari** e di fissazione dell'udienza in camera di consiglio da parte del giudice per le indagini preliminari, in caso di mancato accoglimento dell'istanza (***lettera b***);
- **introduce** all'articolo **407, comma 2, lettera a),** il **numero 7-*ter***, in tal modo estendendo ai delitti informatici 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, il regime che amplia a due anni il **termine per le indagini preliminari**, qualora il fatto sia 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 (***lettera c).***

Quale naturale sviluppo dell'aggravamento del trattamento sanzionatorio per i reati informatici e del rafforzamento degli strumenti investigativi per il relativo contrasto, è stata prevista l'**estensione della disciplina dei collaboratori di giustizia** (articolo 13) **e dei testimoni di giustizia** (articolo 16) agli autori dei reati informatici per i quali l'articolo 2-bis del decreto-legge 10 agosto 2023, n. 105, convertito con modificazioni dalla legge 9 ottobre 2023, n. 137, ha recentemente attribuito il coordinamento al procuratore nazionale antimafia e antiterrorismo.

L'**articolo 13** dello schema, in particolare, modifica l'articolo 9 comma 2, del decreto-legge 15 gennaio 1991, n. 8, convertito, con modificazioni, dalla legge 15 marzo 1991, n. 82, consentendo così l'adozione, per gli autori dei reati informatici previsti al comma 4-bis dell'articolo 371-bis, delle **speciali misure di protezione riservate ai soggetti che**

abbiano collaborato nell'ambito di un procedimento penale, rendendo dichiarazioni qualificate ai sensi del comma 3 del medesimo articolo (intrinseca attendibilità, carattere di novità e completezza, di notevole importanza per lo sviluppo delle indagini, etc.; ***lettera a***).

Viene modificato, quindi, l'articolo 11, comma 2 dello stesso decreto-legge, prevedendo che per i reati informatici di cui all'articolo 371-bis, comma 4-bis, sia effettuata la comunicazione della **proposta di ammissione** alle speciali misure di protezione al procuratore nazionale antimafia e antiterrorismo, ampliando altresì la cognizione di quest'ultimo sui contrasti nel caso di più uffici del pubblico ministero che procedono a indagini collegate (***lettera b***).

Infine, si modifica l'articolo 16-novies, comma 1, del medesimo decreto-legge, estendendo alle persone condannate per i reati informatici attribuiti dall'articolo 371-bis, comma 4-bis al coordinamento del procuratore nazionale antimafia e antiterrorismo, la disciplina speciale dei **benefici penitenziari** riservati dalla legge ai soggetti che collaborano con la giustizia (***lettera c***).

Lo schema di disegno di legge, in un'ottica di sistema, all'**articolo 16** si dà carico di estendere anche la disciplina recante le disposizioni per la **protezione dei testimoni di giustizia** prevedendo, con la modifica dell'articolo 11, comma 2, della legge 11 gennaio 2018, n. 6, che la proposta di ammissione alle speciali misure di protezione possa riguardare anche i reati informatici di cui all'articolo 371-*bis*, comma 4-*bis*, in ordine ai quali è dunque previsto il parere del procuratore nazionale antimafia e antiterrorismo.

Nella prospettiva del potenziamento degli strumenti investigativi, l'**articolo 14**, modifica l'articolo 13 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, inserendo un comma 3-*bis* che estende la **disciplina delle intercettazioni** prevista per i fatti di criminalità organizzata ai reati informatici rimessi dall'articolo 371-*bis* al coordinamento del procuratore nazionale antimafia e antiterrorismo.

La disciplina prevede che le intercettazioni possano autorizzate dal giudice per le indagini preliminari sulla base di sufficienti indizi di reato, quando necessarie per la prosecuzione delle indagini, per un termini di quaranta giorni, suscettibile di proroga per ulteriori periodi di venti giorni.

L'**articolo 15** interviene, poi, in materia di **responsabilità amministrativa degli enti** per gli illeciti dipendenti da reato informatico, modificando sul punto l'articolo 24-*bis* del decreto legislativo 8 giugno 2001, n. 231, con l'innalzamento delle sanzioni previste al comma 1(che passano da un arco edittale compreso tra cento e cinquecento quote, ad un arco compreso tra duecento e settecento quote), l'inserimento di un comma 1-*bis* che prevede la sanzione pecuniaria per la nuova ipotesi di estorsione informatica introdotta all'articolo 629, terzo comma, del codice penale, la previsione di sanzioni pecuniarie al comma 2 per il reato di nuova formulazione previsto all'art. 635-*quater*.1 (per il quale è

innalzata la sanzione sino a quattrocento quote) ed infine la previsione, al comma 4 dello stesso articolo, delle sanzioni interdittive di cui all'articolo 9, comma 2, nei casi di condanna per il delitto indicato nel citato comma 1-*bis*.

Il quadro illustrato trova completamento all'**articolo 17** dello schema, con la regolazione dei **rapporti tra l'Agenzia per la cybersicurezza nazionale** (di seguito ACN), **il procuratore nazionale antimafia e antiterrorismo, la polizia giudiziaria ed il pubblico ministero**, realizzata intervenendo sull'articolo 17 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109 (decreto che, come noto, definisce l'architettura nazionale della cybersicurezza e istituisce l'ACN).

Viene prevista, in particolare, la **trasmissione immediata delle notifiche di incidente** (con un novellato comma 4 dell'articolo 17) da parte del personale dell'Agenzia addetto al 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; la rapida informazione è funzionale a che l'obbligo di denuncia, in tal modo assolto da parte dell'ACN, consenta al pubblico ministero di ricevere tempestivamente la notizia di reato e, assunta la direzione delle indagini, valutare (comma 4-*bis*.3 dell'articolo 17):

a) la **compatibilità degli accertamenti investigativi** con le attività di ripristino dell'ACN di cui all'articolo 7, lett. n- *bis*) del decreto-legge 14 giugno 2021, n. 82 (recentemente introdotto dall'articolo 2-bis del decreto-legge 10 agosto 2023, n. 105, convertito con modificazioni dalla legge 9 ottobre 2023, n. 137);

b) l'attivazione del **raccordo informativo** tra l'organo centrale predetto e l'ACN;

c) l'eventuale **differimento delle attività di ripristino**.

La disciplina introduce inoltre reciproci obblighi informativi tra l'ACN e l'autorità giudiziaria, funzionali ad assicurare l'efficace e tempestivo svolgimento delle attività di ripristino, l'assicurazione delle fonti di prova ed il coordinamento del procuratore nazionale antimafia e antiterrorismo per i reati indicati nel novellato articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale.

In particolare, l'**Agenzia informa senza ritardo il procuratore nazionale antimafia** e antiterrorismo della notizia di un attacco qualificato (comma 4-*bis*.1 dell'articolo 17); corrispondentemente il **pubblico ministero dà tempestiva informazione all'ACN** della notizia dei delitti di cui all'articolo 371-bis, comma 4-*bis*, del codice di procedura penale (comma 4-*bis*.2 dell'articolo 17).

Viene, infine, introdotta la facoltà per l'ACN, in caso di **accertamenti tecnici irripetibili** per i delitti di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale, di assistere al conferimento dell'incarico e partecipare agli accertamenti, anche quando si procede nelle forme dell'incidente probatorio (comma 4-*bis*.4).

L’**articolo 18**, rubricato “Disposizioni finanziarie”, reca, al comma 1, la clausola di invarianza finanziaria stabilendo che dall’attuazione delle disposizioni di cui alla presente legge non devono derivano nuovi o maggiori oneri per il bilancio dello Stato e che le amministrazioni pubbliche interessate provvedono all'adempimento delle disposizioni della presente legge con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente. Il comma 2 dispone che i proventi delle sanzioni di cui all’articolo 1, comma 5, confluiscono tra le 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.

RELAZIONE TECNICA

Il presente provvedimento, finalizzato a rispondere alla crescente offensività delle aggressioni realizzate con mezzi telematici e informatici e alla conseguente esigenza di realizzare una più intensa tutela della sicurezza cibernetica, è composto da **diciotto** articoli, dei quali verranno analizzati, qui di seguito, i relativi profili finanziari.

La parte relativa al Capo I, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale, resilienza delle pubbliche amministrazioni, personale e funzionamento dell'Agenzia per la cybersicurezza nazionale, nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici", contiene disposizioni concernenti la cybersicurezza nazionale finalizzate a conseguire una più elevata capacità di protezione e risposta di fronte a emergenze cibernetiche.

L'**articolo 1** richiede alle pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, alle regioni e alle province autonome di Trento e Bolzano, ai comuni con una popolazione superiore ai 100.000 abitanti e, comunque, ai comuni capoluoghi di regione, nonché alle società di trasporto pubblico urbano con bacino di utenza non inferiore ai 100.000 abitanti e alle aziende sanitarie locali, di segnalare e notificare gli incidenti indicati nella tassonomia di cui all'articolo 1, comma 3-bis, del decreto-legge 21 settembre 2019, n. 105, aventi impatto su reti, sistemi informativi e servizi informatici di pertinenza. Sono tenute alla segnalazione e alla notifica anche le società *in house* di cui si avvalgono i richiamati soggetti.

Dall'inosservanza dell'obbligo di notifica di cui al presente articolo, consegue una preliminare comunicazione dell'Agenzia per la cybersicurezza nazionale all'interessato, che la reiterazione dell'inosservanza comporterà l'applicazione delle sanzioni indicate nel successivo comma 5, e in ispezioni da parte dell'Agenzie medesima cibernetica, anche al fine di verificare l'attuazione degli interventi di rafforzamento della resilienza loro direttamente indicati dall'Agenzia, ovvero previsti da apposite linee guida adottate dalla stessa. Le modalità di tali ispezioni saranno disciplinate con determina del direttore generale dell'Agenzia, pubblicata nella Gazzetta Ufficiale della Repubblica italiana. Per i casi di reiterata inosservanza dell'obbligo di notifica, l'Agenzia per la cybersicurezza nazionale potrà applicare una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000. La violazione delle disposizioni di cui al comma 1 può costituire causa di responsabilità disciplinare e amministrativo-contabile.

Infine, è prevista l'esclusione dall'ambito di applicazione dei richiamati obblighi, fermi gli obblighi e le sanzioni, anche penali, previsti da altre norme di legge, dei soggetti di cui di cui all'articolo 3, comma 1, lettere g) e i), del decreto legislativo n. 65 del 2018 (c.d. soggetti NIS), di quelli di cui all'articolo 1, comma 2-bis, del decreto-legge n. 105 del 2019 (c.d. soggetti Perimetro), nonché degli organi dello Stato preposti alla prevenzione, accertamento e repressione dei reati, alla tutela dell'ordine e della sicurezza

pubblica e alla difesa e sicurezza militare dello Stato, e degli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124.

Le predette disposizioni non comportano nuovi o maggiori oneri a carico della finanza pubblica. ***Le amministrazioni pubbliche interessate provvedono all'adempimento delle disposizioni del presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.***

Con specifico riferimento alle sanzioni previste al comma 5, ferma restando la funzione della misura volta unicamente alla tutela dell'interesse pubblico e l'impossibilità di esprimere una previsione in merito all'eventuale gettito, si evidenzia che le stesse sono di nuova introduzione e che rappresentano entrate rientranti tra quelle di cui all'articolo 11, comma 2, lettera f), del decreto-legge n. 82 del 2021.

L'**articolo 2** stabilisce un obbligo, riferito ai soggetti indicati nel comma 1 dell'articolo 1 del presente provvedimento, nonché ai soggetti Perimetro, ai soggetti NIS, e ai soggetti di cui all'articolo 40, comma 3, alinea, del decreto legislativo 1° agosto 2003, n. 259, di adottare gli interventi risolutivi in conseguenza delle segnalazioni che l'Agenzia per la cybersicurezza nazionale effettua circa specifiche vulnerabilità cui tali soggetti risultano potenzialmente esposti.

È prevista l'applicazione di sanzioni per la mancata o ritardata adozione dei richiamati interventi, nonché una causa di esclusione dall'applicazione delle stesse sanzioni nel caso in cui motivate esigenze di natura tecnico-organizzativa, tempestivamente comunicate all'Agenzia per la cybersicurezza nazionale, impediscano l'adozione degli interventi opportuni o ne comportino il differimento oltre il termine indicato.

Le predette disposizioni non comportano nuovi o maggiori oneri a carico della finanza pubblica. ***Le amministrazioni pubbliche interessate provvedono all'adempimento delle disposizioni del presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.***

Le sanzioni previste al comma 2, come già precisato, rappresentano entrate di cui all'articolo 11, comma 2, lettera f), del decreto-legge n. 82 del 2021.

L'**articolo 3** modifica l'articolo 1, comma 3-bis, del decreto-legge n. 105 del 2019, per finalità di raccordo e coordinamento con le disposizioni recate dal presente provvedimento. In particolare, si prevede, anche per i soggetti Perimetro, l'applicazione della medesima procedura – che consta delle due distinte fasi della segnalazione e della notifica – nonché degli stessi termini, introdotti dall'articolo 1 del presente provvedimento, in relazione alle ipotesi di notifica già previste per gli stessi soggetti Perimetro dal richiamato comma 3-bis, e cioè in relazione a quegli incidenti aventi impatto su reti, sistemi informativi e servizi informatici, di pertinenza di tali soggetti, diversi da quelli inseriti nel Perimetro. È stata, conseguentemente, prevista l'applicazione delle medesime sanzioni introdotte dall'articolo 1 del presente provvedimento per i casi di reiterata violazione dell'obbligo di notifica.

Le predette disposizioni non comportano nuovi o maggiori oneri a carico della finanza pubblica.

Le sanzioni previste rappresentano entrate di cui all'articolo 11, comma 2, lettera f), del decreto-legge n. 82 del 2021

L'**articolo 4** prevede una specifica modalità di funzionamento del Nucleo per la cybersicurezza di cui all'articolo 8 del decreto-legge 14 giugno 2021, n. 82, in relazione a specifiche questioni di particolare rilevanza concernenti i compiti di proposta di iniziative in materia di cybersicurezza del Paese. In particolare, è prevista la possibile convocazione del Nucleo con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati, 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 n. 105 del 2019, nonché di eventuali altri soggetti, interessati alle stesse questioni.

Le disposizioni su illustrate non comportano nuovi o maggiori oneri a carico della finanza pubblica. ***Le amministrazioni pubbliche interessate provvedono all'adempimento delle disposizioni del presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.***

L'**articolo 5** stabilisce la possibilità di differire le attività di resilienza previste dall'articolo 7, comma 1, lettere n) ed n-bis), del decreto-legge n. 82 del 2021, nei casi in cui i servizi di cui agli articoli 6 e 7 della legge 3 agosto 2007, n. 124, avuta notizia di un evento o un incidente informatici, lo ritengano strettamente necessario per motivi legati al perseguimento delle finalità istituzionali del Sistema di informazione per la sicurezza della Repubblica. Di tale necessità, i predetti servizi, per il tramite del Dipartimento delle informazioni per la sicurezza, ne danno informazione al Presidente del Consiglio dei ministri, oppure, laddove istituita, all'Autorità delegata di cui all'articolo 3 della medesima legge n. 124 del 2007.

Nei richiamati casi, è previsto che 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, possa disporre il differimento degli obblighi informativi cui è in ogni caso tenuta l'Agenzia medesima, ai sensi delle disposizioni vigenti, ivi inclusi 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.

Tali disposizioni non comportano nuovi o maggiori oneri a carico della finanza pubblica. ***Le amministrazioni pubbliche interessate provvedono all'adempimento delle disposizioni del presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.***

L'**articolo 6** reca norme che mirano al rafforzamento della resilienza delle pubbliche amministrazioni, proseguendo, in tal modo, nella realizzazione dell'obiettivo anticipato con la direttiva presidenziale del 6 luglio 2023.

In particolare, l'articolo 6 stabilisce che le pubbliche amministrazioni indicate nell'articolo 1, comma 1, del presente provvedimento, debbano provvedere a individuare, laddove non già presente, una struttura, anche tra quelle esistenti, preposta alle relative attività di cybersicurezza e presso la quale opererà la istituenda figura del referente per la cybersicurezza, che svolge, tra l'altro, la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale.

Sono esclusi dall'ambito di applicazione dei richiamati obblighi i soggetti di cui all'articolo 1, comma 2-bis, del decreto-legge n. 105 del 2019 (soggetti Perimetro), per i quali continuano a trovare applicazione gli obblighi previsti dalle disposizioni di cui alla richiamata disciplina, nonché degli organi dello Stato preposti alla prevenzione, accertamento e 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.

Le richiamate disposizioni non comportano nuovi o maggiori oneri a carico della finanza pubblica. ***Le amministrazioni pubbliche interessate provvedono all'adempimento delle disposizioni del presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.***

Con riferimento alla figura del referente per la cybersicurezza previsto al comma 2, si precisa che il relativo incarico non dà diritto a compensi aggiuntivi.

L'**articolo 7** modifica l'articolo 7, comma 1, del decreto-legge 14 giugno 2021, n. 82, inserendo la lettera m-quater), finalizzata a prevedere, in ragione del ruolo di Autorità nazionale per la cybersicurezza, la possibilità per l'Agenzia di promuovere e sviluppare ogni iniziativa, anche di partenariato pubblico-privato, per la valorizzazione dell'intelligenza artificiale come risorsa per il rafforzamento della sicurezza e della resilienza cibernetiche nazionali, anche al fine di favorire un uso etico e corretto dei sistemi basati su tale tecnologia.

Le richiamate disposizioni non comportano nuovi o maggiori oneri a carico della finanza pubblica. ***Le amministrazioni pubbliche interessate provvedono all'adempimento delle disposizioni del presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.***

L'**articolo 8** modifica l'articolo 17 del decreto-legge 14 giugno 2021, n. 82 prevedendo la possibilità di adottare 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, un regolamento per la disciplina del procedimento sanzionatorio amministrativo dell'Agenzia per la cybersicurezza nazionale che stabilisca, in particolare, termini e modalità per l'accertamento, la contestazione e la notifica delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia ai sensi del citato decreto-legge n. 82 del 2021 e

delle altre disposizioni che assegnano poteri accertativi e sanzionatori all'Agenzia. Fino all'entrata in vigore di tale regolamento, da adottarsi entro 90 giorni dalla data di entrata in vigore della presente legge, ai procedimenti sanzionatori si applicano, per ciascuna delle richiamate fasi procedimentali (accertamento, contestazione e notifica delle violazioni della normativa in materia di cybersicurezza e irrogazione delle relative sanzioni), le disposizioni contenute nel capo I, sezioni I e II, della legge 24 novembre 1981, n. 689.

Le su illustrate disposizioni non comportano nuovi o maggiori oneri a carico della finanza pubblica. ***Le amministrazioni pubbliche interessate provvedono all'adempimento delle disposizioni del presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.***

Relativamente ai potenziali effetti finanziari correlati alla disciplina del sistema sanzionatorio si evidenzia che, ai sensi dell'articolo 18, comma 4, del decreto-legge n. 82 del 2021, i proventi di cui all'articolo 11, comma 2, sono versati all'entrata del bilancio dello Stato, per essere riassegnati al capitolo di bilancio istituito nello stato di previsione del Ministero dell'economia e delle finanze e destinato al finanziamento dell'attività dell'Agenzia per la cybersicurezza nazionale.

L'**articolo 9** stabilisce un divieto, della durata di due anni, di assunzione, anche di incarichi, presso soggetti privati finalizzata allo svolgimento di mansioni in materia di cybersicurezza per i dipendenti appartenenti al ruolo del personale dell'Agenzia che abbiano partecipato, nell'interesse e a spese dell'Agenzia, a specifici percorsi formativi di specializzazione. Il medesimo articolo 9 prevede specifiche cause di esclusione dall'applicazione del richiamato divieto nel caso di collocamento a riposo d'ufficio, di raggiungimento del requisito anagrafico previsto dalla legge per la pensione di vecchiaia, di cessazione a domanda per inabilità, ovvero di dispensa dal servizio per motivi di salute. I percorsi formativi di specializzazione che danno luogo al predetto divieto di assunzione, sono individuati con determina del direttore generale dell'Agenzia, che tenga conto della particolare qualità dell'offerta formativa, dei costi, della durata e del relativo livello di specializzazione che consegue alla frequenza dei suddetti percorsi.

Tali disposizioni non comportano nuovi o maggiori oneri a carico della finanza pubblica.

L'**articolo 10** reca disposizioni dirette a indicare criteri di cybersicurezza in tema di appalti. In particolare, è prevista l'adozione di un decreto del Presidente del Consiglio dei ministri, entro 120 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 cybersicurezza di cui all'articolo 4 del decreto-legge 14 giugno 2021, n. 82, con cui sono individuati gli elementi essenziali di cybersicurezza da tenere in considerazione in relazione alle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici.

Le disposizioni dettate mirano a promuovere maggiore garanzia delle esigenze di cybersicurezza, nel caso in cui le attività di approvvigionamento siano connesse alla tutela

degli interessi nazionali strategici. Le richiamate disposizioni vengono coordinate con quanto stabilito dal decreto-legge n. 105 del 2019 per i casi ivi previsti di approvvigionamento di prodotti, processi, servizi ICT e associate infrastrutture destinati alle reti, ai sistemi informativi e per l'espletamento dei servizi informatici conferiti nel perimetro di sicurezza nazionale cibernetica.

Tali disposizioni non comportano nuovi o maggiori oneri a carico della finanza pubblica.

Il Capo II, articoli 11-18, reca, invece, le «*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*». L'articolo 18 contiene la clausola di invarianza finanziaria.

Con l'***articolo 11*** si introducono modifiche al codice penale.

Le disposizioni di cui alla ***lettera a)*** modificano l'articolo 615-*ter* c.p., che disciplina il reato di «*Accesso abusivo ad un sistema informatico o telematico*». Al **numero 1)** si prevedono modifiche al comma secondo dell'articolo: il *punto 1.1* aumenta la pena edittale per le ipotesi aggravate del reato, precedentemente fissata nella reclusione da uno a cinque anni, ora fissata «*da due a dieci anni*»; il *punto 1.2* modifica il numero 2) introducendo all'ipotesi aggravata di esecuzione del reato l'uso di minaccia oltre che con violenza sulle cose o alle persone; il *punto 1.3* qualifica come aggravata la condotta di chi sottrae, anche mediante riproduzione o trasmissione, ovvero renda inaccessibili al titolare, i dati, le informazioni o i programmi contenuti nel sistema informatico o telematico. Il **numero 2)** apporta modifiche al comma terzo dell'articolo 615-*ter* c.p., riguardante i casi in cui i fatti di cui ai precedenti 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. Al *punto 2.1* è aumentata la pena edittale per tali fattispecie aggravate, precedentemente fissata nella reclusione «*da uno a cinque anni e da tre a otto anni*», alla reclusione «*da tre a dieci anni e da quattro a dodici anni*». Al *punto 2.2* è aggiunto un periodo al comma terzo, nel quale si prevede che nei soli casi in cui concorrono anche le circostanze previste dal numero 3) del secondo comma, le circostanze attenuanti diverse da quelle di cui agli articoli 89 («*Vizio parziale di mente*»), 98 («*Minore degli anni diciotto*») e 623-*quater* (introdotto dal presente provvedimento, di seguito esaminato) non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.
La ***lettera b)*** modifica l'articolo 615-*quater* c.p. recante «*Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici*». Il *numero 1)* amplia (dal «*profitto*» al più generico «*vantaggio*») il dolo specifico previsto per la configurabilità della fattispecie. Il *numero 2)* sostituisce il secondo comma, prevedendo l'ipotesi aggravata punita con la pena della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui al precedente articolo 615-*ter*, secondo comma, numero 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). Il *numero 3)* inserisce un ulteriore comma all'articolo, introducendo un'ulteriore ipotesi aggravata punita con la pena della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-*ter*, terzo comma, primo periodo (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 ***lettera c)*** abroga l'articolo 615-*quinquies* che disciplinava le ipotesi di «*Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*», in ottica di riordino e riallineamento sistematico delle fattispecie.
Alla ***lettera d)*** mediante l'aggiunta di ulteriore comma all'articolo 617-*bis* recante «*Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche*», introducendo l'ipotesi aggravata quando ricorre taluna delle circostanze di cui all'articolo 615-*ter*, secondo comma, numero 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), punita con la reclusione da due a sei anni.
La ***lettera e)*** reca modifiche all'articolo 617-*quater* che disciplina il reato di «*Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*». Il *numero 1)* prevede modifiche al quarto comma, che disciplina le fattispecie aggravate per cui è prevista la procedibilità d'ufficio prevedendo: l'aumento della pena edittale dalla reclusione da tre a otto anni alla reclusione da quattro a dieci anni; la procedibilità d'ufficio, quando il fatto è commesso in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615-*ter*, terzo comma, primo periodo (di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico); l'ipotesi aggravata quando il fatto è commesso 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, contestualmente sopprimendo la disposizione specifica di cui al numero 3). Il *numero 2)* aggiunge un ulteriore comma all'articolo 617-*quater*, relativo al bilanciamento delle circostanze, nel quale si prevede che le circostanze attenuanti diverse da quelle di cui agli articoli 89 («*Vizio parziale di mente*»), 98 («*Minore degli anni diciotto*») e 623-*quater* (introdotto dal presente provvedimento, di seguito esaminato) concorrenti con l'aggravante di cui al quarto comma, numero 1), non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alla predetta aggravante.
Alla ***lettera f)*** si introducono modifiche all'articolo 617-*quinquies* recante «*Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche*». Al *numero 1)* si modifica l'ipotesi aggravata, prevedendo che quando ricorre taluna delle circostanze di cui all'articolo 617-*quater*, quarto comma, numero 2), precedentemente esaminato, la pena è della reclusione da due a sei anni. Al *numero 2)* vengono inseriti ulteriori commi

all'articolo, relativi all'ipotesi aggravata quando ricorre taluna delle circostanze di cui all'articolo 617-*quater*, quarto comma, numero 1) precedentemente modificato, punita con la reclusione da tre a otto anni, nonché al bilanciamento delle circostanze.

La ***lettera g)*** introduce modifiche all'articolo 617-*sexies*, recante la fattispecie di reato «*Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*». Si prevede, nell'ipotesi aggravata di cui al comma secondo, l'aumento della pena edittale della reclusione da uno a cinque anni alla reclusione da tre a otto anni, nonché si introducono norme relative al bilanciamento delle circostanze in sede di calcolo della pena.

La ***lettera h)*** modifica la rubrica del Capo III-*bis* del Titolo XII, precedentemente rubricato «*Disposizioni comuni sulla procedibilità*», eliminando il riferimento alla procedibilità in considerazione delle modifiche di cui alla successiva ***lettera i)***, che introduce l'articolo 623-*quater* relativo a due circostanze attenuanti. Si prevede, in particolare, che 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 circostanze dell'azione, ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità (comma 1). Le pene previste per i suddetti delitti sono invece 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 (comma 2). Non si applica il divieto di cui all'articolo 69, comma 4, c.p. riguardo alla mancata prevalenza delle circostanze attenuanti sulle ritenute circostanze aggravanti, e su qualsiasi altra circostanza per la quale la legge stabilisca una pena di specie diversa o determini la misura della pena in modo indipendente da quella ordinaria del reato.

La ***lettera l)*** inserisce un ulteriore comma all'articolo 629, che disciplina il reato di estorsione. Si inserisce una fattispecie di reato che prevede che 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 nell'ultimo capoverso dell'articolo 628.

Mediante la ***lettera m)*** sono apportate modifiche all'articolo 635-*bis* del codice penale, recante la disciplina del reato di «*Danneggiamento di informazioni, dati e programmi informatici*» prevedendo: l'aumento della pena edittale della reclusione da sei mesi a tre anni alla reclusione da due a sei anni. Con le modifiche al secondo comma dell'articolo si introducono disposizioni relative alle fattispecie aggravate. Si prevede che la pena è della reclusione da tre a otto anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema o se il colpevole per commettere il fatto usa minaccia o violenza, ovvero se è palesemente armato.

La ***lettera n)*** apporta modifiche all'articolo 635-*ter* relativo a «*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico*

o comunque di pubblica utilità», prevedendo che nella rubrica, le parole: «*utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*» siano sostituite dalle più generiche: «*pubblici o di interesse pubblico*», aumentando la pena edittale della reclusione da uno a quattro anni alla reclusione da due a sei anni e prevedendo, mediante la sostituzione integrale dei commi secondo e terzo, ulteriori ipotesi aggravate. In particolare, la pena è della reclusione da tre a otto anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; o se il colpevole per commettere il fatto usa minaccia o violenza, ovvero se è palesemente armato; o ancora, 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 in ipotesi di concorrenza delle circostanze aggravanti di cui al precedente comma; in tal caso le circostanze attenuanti diverse da quelle di cui agli articoli 89 («*Vizio parziale di mente*»), 98 («*Minore degli anni diciotto*») e 639-*ter* (introdotto dal presente provvedimento, di seguito esaminato) non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti. Infine, viene modificata la rubrica che prende la seguente denominazione *"Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico"*.

La ***lettera o)*** modifica l'articolo 635-*quater* recante la disciplina della fattispecie di reato «*Danneggiamento di sistemi informatici o telematici*» aumentando la pena edittale della reclusione da uno a cinque anni alla reclusione da due a sei anni e prevedendo, mediante la sostituzione integrale del comma secondo, ulteriori ipotesi aggravate. In particolare, si prevede che la pena è della reclusione da tre a otto anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema, o se il colpevole per commettere il fatto usa minaccia o violenza, ovvero se è palesemente armato.

La ***lettera p)*** inserisce l'articolo 635-*quater*.1, recante «*Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*». Si prevede che chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329. 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) (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). 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, primo periodo (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 ***lettera q)*** sostituisce integralmente l'articolo 635-*quinquies* recante il reato di «*Danneggiamento di sistemi informatici o telematici di pubblico interesse*». Si prevede che salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-*bis* (Danneggiamento di informazioni, dati e programmi informatici), ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, compie atti diretti a distruggere, danneggiare, 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 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; se il colpevole per commettere il fatto usa minaccia o violenza, ovvero se è palesemente armato; 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 in ipotesi di concorrenza delle circostanze aggravanti di cui al precedente comma; in tal caso le circostanze attenuanti diverse da quelle di cui agli articoli 89 («*Vizio parziale di mente*»), 98 («*Minore degli anni diciotto*») e 639-*ter* (introdotto dal presente provvedimento, di seguito esaminato) non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.
La ***lettera r)*** introduce una circostanza attenuante mediante l'articolo 639-*ter* che prevede che 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 circostanze dell'azione, ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità (comma 1). Le pene previste per i suddetti delitti sono invece 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 (comma 2). Non si applica il divieto di cui all'articolo 69, comma 4, c.p. riguardo alla mancata prevalenza delle circostanze attenuanti sulle ritenute circostanze aggravanti, e su qualsiasi altra circostanza per la quale la legge stabilisca una pena di specie diversa o determini la misura della pena in modo indipendente da quella ordinaria del reato.
Dal punto di vista finanziario, si evidenzia che le disposizioni di modifica del codice penale introdotte dall'articolo 1 del presente provvedimento hanno carattere ordinamentale e precettivo e non sono suscettibili di determinare nuovi o maggiori oneri a carico della finanza pubblica.

Con l'***articolo 12*** si introducono modifiche al codice di procedura penale.

In particolare, la disposizione interviene sull'elenco dei reati contenuti nell'art. 51, comma 3-*quinquies* del codice di procedura penale per i quali è competente a procedere la Procura della Repubblica presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente. Con *la **lettera a)*** si sopprime l'art. 615-*quinquies*, abrogato con l'articolo 1, mentre si introducono due fattispecie delittuose che lo sostituiscono e meglio individuano le condotte illecite, vale a dire gli articoli 635-*quater.1* e 635-*quinquies* c.p., articoli anch'essi rispettivamente introdotti e sostituiti dal precedente articolo. Inoltre, viene elencato di seguito a questi il reato 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 cui è estesa la competenza procedurale per identità di materia, trattandosi di sanzionare condotte omissive o elusive, che ostacolano l'emersione di tali reati commessi attraverso strumenti informatici.
Con la ***lettera b)*** e la ***lettera c)*** sono integrati gli articoli 406 e 407 c.p.p. inserendo l'eccezione alla previsione alle modalità operative di comunicazione della proroga dei termini delle indagini preliminari richiesta dal p.m. nonché alla notifica della concessione di tale proroga: infatti quando i reati di cui si sta discutendo sono commessi 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, la durata massima delle indagini è di due anni e la richiesta di proroga dei termini intermedi non deve essere notificata agli indagati.
Dal punto di vista finanziario, si evidenzia che le disposizioni di modifica del codice di procedura penale introdotte dall'articolo 12 del presente provvedimento hanno carattere ordinamentale e procedurale e non sono suscettibili di determinare nuovi o maggiori oneri a carico della finanza pubblica, in quanto le attività espletate dal personale amministrativo e di magistratura riguardano funzioni istituzionali e sono già espletate per reati di pari gravità o di analogo pericolo, preventivi e repressivi di comportamenti lesivi per l'ordine e la sicurezza nazionale.

Con l'***articolo 13*** si introducono modifiche al D.L. 8/1991, convertito, con modificazioni, dalla L. 82/1991. Nella specie, con il **comma 1** ***(lettere a, b e c)*** sono estese anche agli autori dei reati informatici modificati o introdotti con il presente provvedimento, i quali collaborando con l'autorità giudiziaria si trovino in grave pericolo per le forme di cooperazione attivate o le dichiarazioni rilasciate, le speciali misure di protezione e i benefici penitenziari previste dalla predetta legge per i collaboratori ed i testimoni di giustizia. È, inoltre precisato che spetta al Procuratore Nazionale Antimafia e Antiterrorismo esercitare le funzioni di impulso nei confronti dei procuratori distrettuali competente per i predetti reati informatici, al fine di rendere effettivo il coordinamento delle attività di indagine, di garantire la funzionalità dell'impiego della polizia giudiziaria nelle sue diverse articolazioni e di assicurare la completezza e tempestività delle investigazioni.
La disposizione, che organizza le attività degli uffici del pubblico ministero e attribuisce la competenza al Procuratore DNAA per coordinare le indagini tra le procure distrettuali - situazione che si verifica già per altri i reati più gravi di sovversione e pericolo dell'ordine pubblico - ha carattere procedurale e non è suscettibile di determinare un aggravio di oneri per la finanza pubblica.

Con l'***articolo 14*** si modifica l'articolo 13 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, inserendo il nuovo comma 3-*bis* con il quale si prevede che le disposizioni di cui ai commi 1, 2 e 3 del citato decreto relative alla disciplina delle intercettazioni di conversazioni e comunicazioni si applicano anche quando si procede con riferimento ai delitti, consumati o tentati, previsti dall'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale per i quali il procuratore nazionale antimafia e antiterrorismo esercita le funzioni di impulso nei confronti dei procuratori distrettuali e coordinamento dell'attività, come suddetto in relazione al precedente articolo. **La finalità è quella di consentire una più efficace e tempestiva azione diretta all'accertamento delle attività delittuose, prevedendo la possibilità di disporre le operazioni di intercettazione in presenza di sufficienti indizi. Si tratta una modifica ai requisiti procedurali di reperimento della prova, riguardo a fattispecie di reato che mettono in serio pericolo la sicurezza dei sistemi di interesse pubblico e per le quali le intercettazioni sono già previste.**
Dal punto di vista finanziario la norma ha natura procedurale e non è suscettibile di determinare nuovi o maggiori oneri per la finanza pubblica, dal momento che gli adempimenti collegati alle attività istituzionali potranno essere fronteggiati con le ordinarie risorse umane, strumentali e finanziarie disponibili a legislazione vigente, queste ultime iscritte nel bilancio del Ministero della Giustizia, U.d.V. 1.4 – CDR " Dipartimento degli Affari di giustizia "Servizi di gestione amministrativa per l'attività giudiziaria" – Azione "Supporto allo svolgimento dei procedimenti giudiziari attraverso le intercettazioni" – che reca uno stanziamento di euro 212.143.598 per ciascuno degli anni del triennio 2024-2026. ***Si evidenzia inoltre che la recente revisione della disciplina delle intercettazioni con l'adozione dei decreti interministeriali tesi alla razionalizzazione e al contenimento delle tariffe sia delle prestazioni obbligatorie che di quelle funzionali alle operazioni di intercettazione, determinerà risparmi di spesa, come richiesto dal legislatore, assicurando comunque il livello qualitativo dei servizi resi in favore dell'autorità giudiziaria.***

L'***articolo 15*** apporta modificazioni all'articolo 24-*bis* del decreto legislativo 8 giugno 2001, n. 231 in materia di delitti informatici e trattamento illecito dati.
Nel dettaglio la modifica al comma 1 prevede di inasprire la sanzione pecuniaria applicata all'ente che commette i delitti di cui agli articoli 617-*quater*, 617-*quinquies*, 635-bis, 635-*ter*, 635-*quater* e 635-*quinquies* del codice penale, sostituendo le parole "da cento a cinquecento quote" con le parole "da duecento a settecento quote". Sempre in tale ottica di repressione di condotte lesive dell'interesse pubblico si pone l'introduzione del nuovo comma 1-*bis* dopo il comma 1 con il quale si prevede di applicare all'ente la sanzione pecuniaria da trecento a ottocento quote nel caso di commissione del delitto di cui all'articolo 629, terzo comma, del Codice penale.
Con la modifica al comma 2 del citato articolo 24-*bis*, viene sostituito il riferimento all'articolo 615-*quinquies* c.p. a seguito dell'abrogazione di cui si è detto all'articolo 1, con quello all'articolo 635.*quater.1* c.p. e la sanzione pecuniaria viene elevata da trecento a quattrocento quote.

Infine, con l'intervento sul comma 4 del citato articolo, dopo il primo periodo s'inserisce un ulteriore periodo con in quale si prevede che nei casi di condanna per il delitto indicato nel comma 1-*bis* si applicano le sanzioni interdittive previste dall'articolo 9, comma 2 del D.lgs. 231/2000 per una durata non inferiore a due anni.
L'intervento normativo ha natura ordinamentale e precettiva e non presenta profili di onerosità per la finanza pubblica, considerato che le disposizioni sono tese a sanzionare in maniera più incisiva comportamenti che si concretizzano in fattispecie delittuose quali intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, la detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche, il danneggiamento di informazioni, dati e programmi informatici e il danneggiamento di sistemi informatici o telematici di pubblica utilità, generando possibili effetti positivi per la finanza pubblica dovuti all'incremento delle sanzioni pecuniarie, sebbene allo stato non quantificabili.

Con l'***articolo 16*** si apportano modifiche alla legge 11 gennaio 2018, n. 6 ed in particolare sul comma 2 dell'articolo 11, relativo al procedimento di applicazione delle speciali misure di protezione per i testimoni di giustizia e per gli altri protetti, al fine di prevedere che la Commissione centrale richieda il parere al Procuratore nazionale antimafia e antiterrorismo sulla proposta di ammissione alle speciali misure, non solo per le fattispecie delittuose di cui all'articolo 51, commi 3-*bis*, 3-*ter* e 3-*quater*, del codice di procedura penale, ma anche nel caso di delitti di cui all'articolo 371-*bis*, comma 4-*bis* del codice di procedura penale.
La norma ha natura ordinamentale e procedurale e non è suscettibile determinare nuovi o maggiori oneri per la finanza pubblica, atteso che tali adempimenti rientrano fra le ordinarie attività istituzionali e pertanto, potranno essere garantite con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

L'***articolo 17*** interviene sul decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109 relativo alle "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"*.
Al riguardo si prevede la sostituzione del comma 4 dell'articolo 17 del citato decreto-legge e l'inserimento di quattro nuovi commi (4-bis.1; 4-bis.2; 4-bis.3 e 4-bis.4), al fine di meglio regolare i rapporti fra le diverse autorità coinvolte (Agenzia per la cybersicurezza nazionale, procuratore nazionale antimafia e antiterrorismo, la polizia giudiziaria e il pubblico ministero.
Il comma 4 viene completamente sostituito, ribadendo che il personale dell'Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni, riveste la qualifica di pubblico ufficiale e prevedendo che la trasmissione delle notifiche di incidente ricevute dal CSIRT Italia all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 144/2005 deve essere immediata, in quanto costituisce adempimento dell'obbligo

previsto dall'articolo 331 del codice di procedura penale in materia di denuncia da parte dei pubblici ufficiali e incaricati di pubblico servizio.

Con il nuovo comma 4-*bis*.1 si prevede che nei casi in cui l'Agenzia abbia 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 comunque in tutti quei casi in cui risulti coinvolto uno dei soggetti individuati all'articolo 1, comma 2-*bis*, del decreto-legge n. 105/2019 (amministrazioni pubbliche, enti e operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato o dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale), dall'articolo 3, comma 1, lettere g) ed i) del D.lgs. 65/2018 (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 del citato decreto legislativo e fornitore di servizio digitale), dall'articolo 40, comma 3 alinea, del decreto legislativo 1° agosto 2003, n. 259 (imprese reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, fermo restando quanto previsto dal comma 4, procede alle attività di cui all'articolo 7, comma 1, lettere n) e n-*bis*) che sono indispensabili per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, nonché il ripristino dell'operatività dei sistemi compromessi e ne informa senza ritardo il procuratore nazionale antimafia e antiterrorismo, ai sensi del comma 4-*bis*.

Con il successivo comma 4-*bis*.2 si prevede che fuori dai casi previsti dal precedente comma, il pubblico ministro sia tenuto ad informare tempestivamente l'Agenzia della cybersicurezza quando acquisisce la notizia dei delitti di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale.

Il comma 4-*bis*.3 prevede che il pubblico ministero nell'impartire le disposizioni necessarie ad assicurare gli accertamenti urgenti tenga conto delle attività di analisi e prevenzione svolte dall'Agenzia per la cybersicurezza nazionale, potendo con decreto motivato altresì differire una o più delle predette attività se ritiene che le stesse possano creare un pregiudizio al corso delle indagini. Si prevede, inoltre, che il pubblico ministero assicuri il necessario collegamento informativo con l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, al fine di assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate (articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155).

Infine, con il comma 4-*bis*.4 viene previsto, in caso di accertamenti irripetibili, la facoltà per l'Agenzia per la cybersicurezza nazionale di assistere al conferimento dell'incarico e partecipare agli accertamenti, anche quando si procede nelle forme dell'incidente probatorio.

Dal punto di vista finanziario si segnala che le disposizioni esaminate hanno natura ordinamentale e procedurale e non determinano nuovi o maggiori oneri a carico della

finanza pubblica, in quanto sono tese ad attivare un raccordo informativo fra i diversi soggetti, a introdurre reciproci obblighi informativi fra i predetti soggetti, a rendere compatibili le attività del pubblico ministero (accertamenti investigativi) con le attività di ripristino della Agenzia per la cybersicurezza nazionale, al fine di rendere più efficace e tempestiva la tutela della sicurezza cibernetica.

L'***articolo 18*** reca la clausola di invarianza finanziaria, prevedendo che *dall'attuazione della presente legge non devono derivare nuovi e maggiori oneri a carico della finanza pubblica. Le amministrazioni pubbliche interessate provvedono all'adempimento delle disposizioni della presente legge con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.*

Il comma 2 dispone che i proventi delle sanzioni di cui all'articolo 1, comma 5, confluiscono tra le 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.

Ministero dell'Economia e delle Finanze

DIPARTIMENTO DELLA RAGIONERIA GENERALE DELLO STATO

VERIFICA DELLA RELAZIONE TECNICA

La verifica della presente relazione tecnica, effettuata ai sensi e per gli effetti dell'art. 17, comma 3, della legge 31 dicembre 2009, n. 196 ha avuto esito Positivo.

Il Ragioniere Generale dello Stato

Firmato digitalmente

15/02/2024