Disegno di legge recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (AS 1143)

RELAZIONE TECNICA

Si premette che la numerazione degli articoli è stata modificata, in quanto la versione originaria era costituita da 18 articoli mentre il testo approvato dall'Assemblea nella Camera dei deputati consta di 24 articoli. distribuiti in 2 Capi, recanti rispettivamente: "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale, di resilienza delle pubbliche amministrazioni e del settore finanziario, di personale e funzionamento dell'Agenzia per la cybersicurezza nazionale, e degli organismi di informazione per la sicurezza nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici*" (articoli da 1 a 15) e "*Disposizioni per la prevenzione e il contrasto dei reati informatici nonché in materia di coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici e di sicurezza delle banche di dati in uso presso gli uffici giudiziari*" (articoli da 16 a 24).

Nello specifico verranno analizzati, qui di seguito, i profili finanziari relativi alle singole disposizioni.

Il presente provvedimento **è** 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.

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.

Al comma 1, tra le pubbliche amministrazioni destinatarie del provvedimento, sono state inserite le città metropolitane, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane ed è stato chiarito che sono altresì destinatarie le società in house che forniscono servizi informatici, i servizi di trasporto ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali. È stato inoltre inserito il nuovo comma 3 il quale dispone che gli obblighi di notifica si applichino per alcuni soggetti a decorrere dal centottantesimo giorno dalla data di entrata in vigore del presente provvedimento. Si tratta di: Comuni con popolazione superiore a 100.000 abitanti; Comuni capoluoghi di Regione; società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti; società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane; aziende sanitarie locali; società in house che forniscono servizi informatici, servizi di trasporto, nonché quelle che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali, ovvero che si occupano della gestione dei rifiuti. I commi 5 e 6 (ex commi 4 e 5) indicano le sanzioni per la violazione dell'obbligo di notifica. Rispetto al testo originario è stato previsto che la reiterazione dell'inosservanza nell'arco di cinque anni comporterà l'applicazione delle sanzioni. Inoltre, è stato specificato nel comma 6 che la violazione delle disposizioni del comma 1 dell'articolo in esame può costituire causa di responsabilità disciplinare e amministrativo-contabile per i funzionari e i dirigenti responsabili.

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 che l'Agenzia debba provvedere all'elaborazione e alla classificazione dei dati relativi alle notifiche di incidenti ricevute. Tali dati sono quindi resi pubblici nell'ambito della relazione prevista dall'articolo 14, comma 1, del decreto-legge n. 82 del 2021.
A tali adempimenti si provvede con le risorse umane, strumentali e finanziarie già previste a legislazione vigente.

La predetta disposizione non comporta, pertanto, nuovi o maggiori oneri a carico della finanza pubblica.

L'**articolo 5** 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 6** 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 7 modifica la composizione del Comitato interministeriale per la sicurezza della Repubblica al fine di prevedere la possibilità di partecipazione a quest'ultimo anche del Ministro dell'agricoltura, della sovranità alimentare e delle foreste, del Ministro delle infrastrutture e dei trasporti e del Ministro dell'università e della ricerca.

Tale disposizione è ordinamentale e non comporta nuovi o maggiori oneri a carico della finanza pubblica.

L'**articolo 8** 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.

Alla lettera b) del comma 1, la struttura istituita, ove non sia già presente, per le pubbliche amministrazioni indicate nell'articolo 1, comma 1, provvede anche alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento. Al comma 2, si aggiunge la previsione che il referente per la cybersicurezza sia individuato in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza. Nel caso in cui i soggetti di cui all'articolo 1, comma 1, non dispongano di personale dipendente fornito di tali requisiti, possono conferire l'incarico di referente per la cybersicurezza a un dipendente di una pubblica amministrazione, previa autorizzazione di quest'ultima ai sensi dell'articolo 53 del decreto legislativo 30 marzo 2001, n. 165, nell'ambito delle risorse disponibili a legislazione vigente. Si introducono, quindi, i commi 3, 4 e 5, prevedendo che la struttura e il referente possano essere individuati nell'ufficio e nel responsabile per la transizione al digitale, previsti dall'articolo 17 del decreto legislativo n. 82 del 2005 (codice dell'amministrazione digitale), e che i loro compiti possano essere esercitati anche in forma associata.

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 9 attribuisce alle strutture ***di cui all'articolo 8 del presente provvedimento, nonché a quelle che svolgono analoghe funzioni per i soggetti di cui all'articolo 1,***

comma 2-bis, del decreto-legge n. 105 del 2019 e al decreto legislativo 18 maggio 2018, n. 656, il compito di verificare che i programmi e le applicazioni informatiche e di comunicazione elettronica in uso (e che utilizzano soluzioni crittografiche), rispettino le linee guida sulla crittografia nonché quelle sulla conservazione delle password adottate dall'Agenzia per la cybersicurezza nazionale e dal Garante per la protezione dei dati personali e che non comportino vulnerabilità note, atte a rendere disponibili e intellegibili a terzi i dati cifrati.

La disposizione non genera nuovi o maggiori oneri per la finanza pubblica. Agli adempimenti previsti si provvede con le risorse umane, strumentali e finanziarie già previste a legislazione vigente.

L'**articolo 10** 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.

Inoltre, viene sostituita la lettera m-bis dell'articolo 7, comma 1, del decreto-legge 14 giugno 2021, n. 82. La modifica valorizza l'utilizzo della crittografia, anche a vantaggio della tecnologia blockchain, quale strumento di difesa cibernetica e istituisce il Centro nazionale di crittografia presso l'Agenzia per la cybersicurezza nazionale. La disposizione istituisce presso l'ACN, l'Agenzia appunto, il Centro nazionale di crittografia, con funzioni di centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato, ossia non coperto dal segreto. Il funzionamento del Centro è disciplinato con provvedimento del direttore generale dell'Agenzia. L'articolo in esame fa salve le competenze dell'Ufficio centrale per la segretezza. Di conseguenza la rubrica è stata modificata in "Funzioni dell'Agenzia per la cybersicurezza nazionale in materia di crittografia".

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 11** 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.

Inoltre, è stata inserita la previsione secondo cui il regolamento per la disciplina del procedimento sanzionatorio amministrativo dell'Agenzia per la cybersicurezza nazionale stabilisce, in particolare, termini e modalità per l'accertamento, da 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 e che su tale regolamento sia acquisito anche il parere delle competenti Commissioni parlamentari.

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 12** 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.

Il comma 2 prevede che fino al 31 dicembre 2026 il requisito di permanenza minima nell'area operativa ai fini del passaggio nell'Area manageriale sia fissato in tre anni.

Quest'ultimo intervento normativo non varia il numero delle unità acquisibili con il concorso, ma definisce la sola platea dei possibili partecipanti. Pertanto, non produce l'effetto di accelerazione di carriera, di conseguenza quello di generare ulteriori spese.

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

L'articolo 13 stabilisce il divieto per coloro che abbiano ricoperto la carica di Direttore generale, di Vice Direttore generale del DIS e di Direttore e di Vice Direttore di AISE o di AISI, ovvero che abbiano svolto incarichi dirigenziali di prima fascia di preposizione a strutture organizzative di livello dirigenziale generale, di svolgere attività lavorativa, professionale, o consulenziale, ovvero ricoprire cariche presso soggetti esteri, pubblici o privati, ovvero presso soggetti privati italiani a cui si applica il decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, nei tre anni successivi alla cessazione dell'incarico, salvo specifica autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità delegata, ove istituita.
Analogo divieto è posto nei confronti del personale di cui al ruolo unico previsto dall'articolo 21 della legge 3 agosto 2007, n. 124, al quale è precluso svolgere attività lavorativa, professionale o consulenziale, ovvero ricoprire cariche, presso enti o privati titolari di licenza ai sensi dell'articolo 134 del TULPS, o comunque presso soggetti che a qualunque titolo svolgano attività di investigazione, ricerca o raccolta informativa.
Lo stesso personale di cui al ruolo unico previsto dall'art. 21 legge 124/2007 che abbia partecipato, nell'interesse e a spese del DIS, dell'AISE o dell'AISI, a specifici percorsi formativi di specializzazione, è fatto divieto di assumere incarichi presso soggetti privati per svolgere le medesime mansioni per le quali ha beneficiato delle suddette attività formative, per la durata di tre anni a decorrere dalla data di completamento dell'ultimo dei predetti percorsi formativi.
I contratti conclusi e gli incarichi conferiti in violazione del citato divieto sono nulli.
Tali disposizioni hanno natura ordinamentale, pertanto non comportano nuovi o maggiori oneri a carico della finanza pubblica.

L'**articolo 14** 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.

Al comma 1 si prevede che** per l'adozione del decreto del Presidente del Consiglio dei ministri entro 120 giorni dalla data di entrata in vigore del provvedimento in esame, su proposta dell'Agenzia per la cybersicurezza nazionale sia necessario il previo parere del Comitato interministeriale per la sicurezza della Repubblica, per individuare, per determinate categorie tecnologiche di beni e servizi, gli elementi essenziali di cybersicurezza. Inoltre si stabilisce che il DPCM **individui anche i casi in cui, per la tutela della sicurezza nazionale, devono essere previsti criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza nazionali o europee di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi individuati con il decreto tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione. Le disposizioni vengono coordinate nel comma 4 con quanto stabilito dal decreto-legge n. 105 del 2019 per i casi ivi previsti di beni, sistemi e servizi di information and communication technology destinati ad essere impiegati nelle reti e nei sistemi informativi nonché per l'espletamento dei servizi informatici di cui alla lettera b) del comma 2 del medesimo articolo.

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

Il Capo I si chiude con l'articolo 15, volto a inserire nell'articolo 16 della legge 21 febbraio 2024, n. 15, cd. legge di delegazione europea 2022-2023, nuovi principi e criteri direttivi specifici a cui il Governo dovrà attenersi nel recepimento della normativa europea in materia di resilienza operativa digitale per il settore finanziario. Le integrazioni aggiungono un nuovo criterio direttivo volto a conseguire un livello elevato di resilienza operativa digitale e assicurare la stabilità del settore finanziario definendo adeguati presìdi in materia di resilienza operativa digitale e attribuendo alla Banca d'Italia l'esercizio nei confronti dei soggetti di cui alla presente lettera dei poteri di vigilanza, di indagine e sanzionatori.

Ai sensi del comma 3 del citato articolo 16 della Legge 15/2024, dall'attuazione del citato articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Prevede altresì che le amministrazioni competenti provvedano all'adempimento dei compiti derivanti dall'esercizio della delega di cui al presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Con l'articolo 16 si introducono modifiche al codice penale.

*Le disposizioni di cui alla **lettera a) intervengono sull'articolo 240, secondo comma, numero 1-bis, allo scopo di sanzionare più rigorosamente le truffe consumate a distanza attraverso l'utilizzo di strumenti informatici, prevede la confisca obbligatoria ai sensi dell'articolo 240, secondo comma, numero 1-bis dei beni e degli strumenti informatici o telematici con i quali è stato perpetrato il reato di cui all'articolo 640, secondo comma, numero 2-ter), sul quale v. infra, lettera t).** Le disposizioni di cui alla **lettera b)** 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.* ***In particolare, è aumentata la misura della 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».***

La ***lettera c)*** *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.*

La ***lettera d)*** *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 e)*** *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 f)*** *reca modifiche all'articolo* ***617-quater, quarto comma,*** *che disciplina il reato di «Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche»,* ***nella forma aggravata. Il numero 1) interviene prevedendo***

l'aumento della pena edittale dalla reclusione da tre a otto anni alla reclusione «da quattro a dieci anni»; il numero 2) prevede 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; il numero 3) disciplina 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; il numero 4) interviene sopprimendo la disposizione specifica di cui al numero 3) dell'articolo 617-quater, quarto comma.

*Alla **lettera g)** 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) viene inserito **un ulteriore comma** 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.*

*La **lettera h)** 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.*

*La **lettera i)** 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 l)**, 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 m)** 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 n)*** *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 o)*** *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 con taluna delle circostanze di cui al numero 3).*** *Infine, viene modificata la rubrica che prende la seguente denominazione "Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico".*
La ***lettera p)*** *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 q)** 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.*

*La **lettera r)** 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 quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3).***

*La **lettera s)** 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.
La lettera t) è diretta a sanzionare più rigorosamente le truffe consumate attraverso l'utilizzo di strumenti informatici, prefigurando così la ricorrenza degli estremi della minorata difesa del contraente più debole, ossia il cliente finale allettato dall'offerta artificiosamente camuffata come vantaggiosa. In tal senso, pertanto, si prevede per tale reato un'ipotesi aggravata (numero 1, che introduce il numero 2-ter al comma secondo dell'articolo 640) e procedibile d'ufficio (numero 2, che interviene sul terzo comma dell'articolo 640), quando il fatto è commesso a distanza mediante strumenti informatici o telematici che ostacolano l'identificazione del proponente.
La lettera u) prevede, mediante la modifica dell'articolo 640-quater, nell'ipotesi di truffa aggravata di cui all'articolo 640, comma secondo, numero 2-ter, appena esaminato, l'applicabilità dell'articolo 322-ter, in materia di confisca obbligatoria dei beni che costituiscono il profitto o il prezzo del reato.

Dal punto di vista finanziario, si evidenzia che le disposizioni di modifica del codice penale hanno carattere ordinamentale e precettivo e non sono suscettibili di determinare nuovi o maggiori oneri a carico della finanza pubblica.

Con l'***articolo 17*** 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 18*** 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 19*** 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 20*** 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 21*** 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 22*** 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 23 pone in essere* modifiche all'articolo 7 della legge 12 agosto 1962, n. 1311, finalizzate a verificare la regolarità degli accessi degli operatori alle banche dati giudiziarie e alle altre banche dati in uso agli uffici giudiziari attraverso l'espletamento programmato delle ispezioni effettuate dall'ispettorato generale presso il Ministero della giustizia ovvero anche nell'ambito delle ispezioni parziali disposte**

dall'amministrazione giudiziaria in caso di necessità o esigenze particolari, al fine di accertare la produttività degli stessi nonché l'entità e la tempestività del lavoro di singoli magistrati.

Gli adempimenti previsti dalla disposizione non generano nuovi o maggiori oneri per la finanza pubblica, in quanto rientrano tra i compiti istituzionali delegati all'organo ispettivo, il quale vi provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

L'***articolo 24*** 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

28/05/2024