nota di lettura

XIX legislatura

A.S. 1143:

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

(Approvato dalla Camera dei deputati)

Maggio 2024
n. 149

servizio del bilancio
del Senato

Senato
della Repubblica

SERVIZIO DEL BILANCIO
Tel. 06 6706 5790 – SBilancioCU@senato.it – 𝕏 @SR_Bilancio

Servizio del bilancio, (2024). Nota di lettura, «A.S. 1143: "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici"». NL149, maggio 2024, Senato della Repubblica, XIX legislatura

I N D I C E

PREMESSA

Al momento del completamento del presente *dossier*, non risulta depositata la relazione tecnica aggiornata ai sensi dell'articolo 17, comma 8, della legge n. 196 del 2009.

Le analisi qui presentate sono state effettuate sulla base delle relazioni tecniche riferite ai singoli emendamenti e sul materiale informativo trasmesso nel corso dell'esame presso la Camera dei deputati.

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

Articolo 1
(Obblighi di notifica di incidenti)

Il comma 1 prevede un obbligo di segnalazione e notifica di alcune tipologie di incidenti aventi impatto su reti, sistemi informativi e servizi informatici in carico ai seguenti soggetti:

- pubbliche amministrazioni centrali incluse nell'elenco annuale ISTAT delle pubbliche amministrazioni previsto dall'articolo 1, comma 3, della legge di contabilità e finanza pubblica (legge n. 196 del 2009);
- regioni e province autonome di Trento e di Bolzano; città metropolitane (soggetti aggiunti in prima lettura);
- comuni con popolazione superiore a 100.000 abitanti e comunque i 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* degli enti fin qui richiamati che siano fornitrici di servizi informatici, dei servizi di trasporto sopra indicati, dei servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali ovvero servizi di gestione dei rifiuti.

Si specifica che gli incidenti da segnalare sono quelli indicati nella tassonomia di cui all'articolo 1, comma 3-*bis*, del decreto-legge n. 105 del 2019. Tale disposizione richiama a sua volta gli incidenti di cui all'articolo 1, comma 1, lettera h) del regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici adottato con il DPCM n. 81 del 2021 e cioè "ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici".

Il comma 2 indica le modalità con le quali effettuare la notifica: una prima segnalazione deve avvenire senza ritardo e comunque entro il termine massimo di ventiquattro ore dal momento in cui ne sono venuti a conoscenza; entro settantadue ore dal medesimo momento dovrà avvenire la notifica completa di tutti gli elementi informativi disponibili. Sia la segnalazione che la notifica completa

dovranno avvenire utilizzando le procedure disponibili sul sito *internet* dell'Agenzia per la cybersicurezza nazionale.

Il comma 3 dispone che gli obblighi di notifica indicati ai precedenti commi (segnalazione degli incidenti e modalità per l'effettuazione della 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 descritti come sopra, nonché quelle che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali, ovvero che si occupano della gestione dei rifiuti. Conseguentemente, gli obblighi di notifica si applicheranno invece a decorrere dalla data di entrata in vigore della presente legge per: le pubbliche amministrazioni centrali incluse nell'elenco annuale ISTAT delle pubbliche amministrazioni previsto dall'articolo 1, comma 3, della legge n. 196 del 2009; le regioni e province autonome di Trento e di Bolzano; le città metropolitane.

Il comma 4 dispone che, i soggetti indicati al comma 1 possono effettuare anche notifiche volontarie di incidenti ulteriori rispetto a quelli oggetto di obbligo di notifica sopra descritti. In tal caso si applica quanto previsto per le notifiche volontarie dai commi 3, 4 e 5 del decreto legislativo n. 65 del 2018 (di recepimento della direttiva (UE) 2016/1148 in materia di sicurezza delle reti e dei sistemi informativi dell'Unione) e cioè che le notifiche volontarie sono trattate successivamente alle notifiche obbligatorie (comma 3); le notifiche volontarie sono trattate solo qualora tale trattamento non costituisca un onere sproporzionato o eccessivo (comma 4); la notifica volontaria non può avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica (comma 5).

Il comma 5 prevede, in caso di inosservanza, la comunicazione da parte dell'Agenzia per la cybersicurezza nazionale all'interessato che la reiterazione dell'inosservanza nell'arco di cinque anni comporterà l'applicazione delle sanzioni previste dal comma 6. In caso di inosservanza l'Agenzia inoltre può disporre ispezioni. Queste ispezioni avranno anche il compito di verificare l'attuazione da parte dei soggetti interessati di interventi di rafforzamento della loro resilienza rispetto al rischio di incidenti, interventi direttamente indicati dall'Agenzia ovvero previsti da apposite linee guida adottate dall'Agenzia. Le modalità di svolgimento delle ispezioni saranno disciplinate con determinazione del direttore generale dell'Agenzia pubblicata nella "Gazzetta Ufficiale".

Il comma 6 individua la sanzione amministrativa pecuniaria per la reiterata inosservanza, nell'arco di cinque anni, dell'obbligo di notifica da un minimo di 25.000 a un massimo di 125.000 euro a carico dei soggetti indicati al comma 1. L'applicazione della sanzione avverrà, specifica la disposizione, nel rispetto "dell'articolo 17, comma 4-quater, del decreto-legge n. 82 del 2021"; tale comma è introdotto dall'articolo 11 del presente provvedimento. La violazione può comunque anche costituire causa di responsabilità disciplinare e amministrativo-contabile nei confronti, come specificato in sede referente, dei funzionari e dei dirigenti responsabili.

Il comma 7, alle lettere a) e b), esclude dall'ambito di applicazione dell'articolo: gli operatori di servizi essenziali per il mantenimento di attività sociali e/o economiche fondamentali in cui la fornitura di tali servizi dipende dalla rete e dai servizi informativi e in cui un incidente avrebbe effetti negativi rilevanti sulla fornitura del servizio, nei settori dell'energia, bancario, finanziario, sanitario, nel settore dell'acqua potabile e nelle infrastrutture digitali (articolo 3, comma 1, lettera g) del decreto legislativo n. 65 del 2018, che a sua volta richiama, per la definizione dei servizi essenziali, l'articolo 4, comma 3, e l'allegato II); i fornitori di servizi digitali (di cui all'articolo 3, comma 1, lettera i) del decreto legislativo n. 65 del 2018);i soggetti già ricompresi nel perimetro di sicurezza nazionale cibernetica di cui all'articolo 1, comma 2-*bis* del decreto-legge n. 105 del 2019; organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa della sicurezza militare dello Stato; il Dipartimento delle informazioni per la sicurezza (DIS) (art. 4, legge n. 124 del 2007); l'Agenzia di informazione e sicurezza esterna (AISE)

(art. 6, legge n. 124 del 2007) e l'Agenzia di informazione e sicurezza interna (AISI) (art. 7, legge n. 124 del 2007).

La RT annessa al DDL iniziale evidenzia che il 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.

Sull'articolo 1 conferma che la norma 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 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.

Il comma 3 e le novelle apportate ai commi 1, 5 e 6 nel corso dell'esame svolto in prima lettura, sono al momento sprovviste di **RT**.

Al riguardo, sulla neutralità delle norme, che secondo la RT non comportano nuovi o maggiori oneri a carico della finanza pubblica, attestata dalla circostanza che le amministrazioni pubbliche interessate dovranno provvedere ai connessi adempimento con le sole risorse umane, strumentali e finanziarie già disponibili nei loro bilanci ai sensi della legislazione vigente, rinviando in generale alla clausola di invarianza dall'articolo 24, si formulano alcune osservazioni.

Dal momento che la disposizione pone obblighi di notifica da eseguire entro brevi termini (24 ore per la prima notifica, 72 ore per la notifica completa a carico di molteplici soggetti pubblici), andrebbe anzitutto assicurato, fornendo specifici elementi informativi, che tali soggetti siano dotati di strutture adeguate.

Inoltre, anche per quanto riguarda la Agenzia per la cybersicurezza nazionale andrebbero forniti maggiori informazioni circa la sua infrastruttura informatica, posto che le notifiche dovranno essere trasmesse tramite le procedure disponibili sul sito *internet*; andrebbero altresì forniti elementi sulla dotazione di personale per lo svolgimento delle attività ispettive e per la ricezione e l'esame delle notifiche, nonché per le istruttorie finalizzate all'applicazione delle sanzioni previste.

Articolo 2
(Mancato o ritardato adeguamento a segnalazioni dell'Agenzia per la cybersicurezza nazionale)

Il comma 1 riconosce all'Agenzia per la cybersicurezza nazionale (ACN) la facoltà di segnalare, ad una serie di soggetti pubblici o che forniscono servizi pubblici, specifiche vulnerabilità cui essi risultano potenzialmente esposti; inoltre prevede che i destinatari di tali segnalazioni devono provvedere senza ritardo, e comunque non oltre 15 giorni dalla comunicazione, all'adozione degli interventi risolutivi indicati dalla stessa Agenzia. La disposizione si applica, oltre che ai soggetti di cui all'articolo 1, comma 1, del provvedimento in commento, ossia quelli tenuti a segnalare all'ACN gli incidenti cibernetici cui sono incorsi (le amministrazioni centrali, le regioni e provincie autonome, i grandi comuni, le grandi società di trasporto pubblico urbano e le ASL) anche ai seguenti soggetti:

- soggetti inclusi nel perimetro di sicurezza nazionale, di cui all'articolo 1, comma 2-*bis*, del D.L. 105/2019: ossia le 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, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale; l'elenco di tali soggetti è contenuto in un atto amministrativo, non soggetto a pubblicazione, adottato dal Presidente del Consiglio, su proposta del Comitato interministeriale per la cybersicurezza - CIC, entro trenta giorni dalla data di entrata in vigore del DPCM che reca

modalità e criteri procedurali di individuazione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica;

- i soggetti NIS, di cui all'articolo 3, comma 1, lettere g) e i), del D.Lgs. 65/2018 (*attuazione direttiva Network and information security - NIS*), ossia: operatori di servizi essenziali, ossia i soggetti pubblici o privati, che forniscono un servizio (dipendente dalla rete e dai sistemi informativi) essenziale per il mantenimento di attività sociali e economiche fondamentali (concernenti settori quali l'energia, i trasporti, banche, sanità, acqua potabile e infrastrutture digitali); fornitori di servizi digitali, cioè qualsiasi persona giuridica che fornisce un servizio digitale, ossia un servizio della società dell'informazione prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi;
- soggetti Tel.Co., di cui all'articolo 40, comma 3, alinea, del D.Lgs. 259/2003 (*codice delle comunicazioni elettroniche*), ossia le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico.

Il comma 2 prevede l'applicazione di una sanzione amministrativa pecuniaria in caso di mancata o ritardata adozione degli interventi risolutivi indicati dall'ACN di cui al comma 1. Si tratta della medesima sanzione per la reiterata inosservanza, nell'arco di cinque anni, dell'obbligo di notifica all'ACN degli incidenti cibernetici indicata all'articolo 1, comma 6, del provvedimento in esame: da 25 mila a 125 mila euro. La sanzione è comminata dall'ACN. La sanzione non si applica nel caso in cui motivate esigenze di natura tecnico-organizzativa, che devono essere tempestivamente comunicate all'Agenzia per la cybersicurezza nazionale, ne impediscano l'adozione o ne comportino il differimento oltre il termine di 15 giorni.

La RT annessa al DDL iniziale conferma che la disposizione 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.

Al riguardo, posto che le norme in esame prefigurano l'obbligo per le pubbliche amministrazioni e i soggetti operanti nel settore dei pubblici servizi di conformarsi alle

indicazioni dell'Agenzia per la cybersicurezza in conseguenza della verifica dei rischi di vulnerabilità informatica, con gli ipotizzabili effetti d'oneri conseguenti alla necessità di adeguamento delle proprie dotazioni *hardware* e *software*, andrebbero forniti elementi di rassicurazione circa l'adeguatezza delle risorse umane e strumentali già previste ai sensi della legislazione vigente nei bilanci di tali Amministrazioni .

Ciò detto, in particolare, alla luce di quanto stabilito dal comma 2, che prevede espressamente l'applicazione di sanzioni per la mancata o ritardata adozione dei richiamati interventi, escluse per sole motivate "esigenze di natura tecnico-organizzativa", da comunicare tempestivamente all'Agenzia per la cybersicurezza nazionale, che impediscano l'adozione degli interventi opportuni o ne comportino il differimento oltre il termine indicato.

Articolo 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)

L'articolo, alle lettere a) e b), stabilisce che i soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica sono tenuti a provvedere, oltre che alla notifica alla ACN, anche alla segnalazione alla medesima degli incidenti che intervengono su reti, sistemi informativi e servizi informatici che si trovano al di fuori del Perimetro (di loro pertinenza), senza ritardo, e comunque al massimo entro ventiquattro ore, con finalità di coordinamento del D.L. n. 105/2019 (c.d. decreto" Perimetro") con le modifiche recate all'articolo 1 del disegno di legge in esame. Con la medesima finalità si prevede altresì l'applicazione della sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000 in caso di reiterata inosservanza dell'obbligo di notifica.

La RT annessa al DDL iniziale conferma che l'articolo 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. La RT conferma che le sanzioni previste rappresentano entrate di cui all'articolo 11, comma 2, lettera f), del decreto-legge n. 82 del 2021.

Al riguardo, posto che le disposizioni prevedono, per i soggetti inseriti nel Perimetro di sicurezza nazionale cibernetica, l'obbligo di effettuare la segnalazione degli incidenti entro il termine massimo di ventiquattro ore, andrebbe data conferma della disponibilità

di adeguate risorse che consentano di rispettare tale breve termine. Si ricorda che già la normativa vigente prevede la notifica entro un termine di 72 ore.

Articolo 4
(Disposizioni in materia di dati relativi a incidenti informatici)

L'articolo integra, inserendo una nuova lettera n-*ter)*, i compiti dell'Agenzia per la cybersicurezza nazionale, come descritti dall'articolo 7, comma 1, del decreto-legge n. 82 del 2021.

In particolare, spetterà d'ora innanzi all'Agenzia provvedere non solo alla raccolta, ma anche alla elaborazione e classificazione dei dati relativi alle notifiche di incidenti informatici, ricevute dai soggetti a ciò tenuti dalle norme vigenti. La pubblicità dei dati sugli incidenti informatici deve essere assicurata nell'ambito della relazione che il Presidente del Consiglio trasmette entro il 30 aprile di ogni anno al Parlamento sull'attività svolta dall'Agenzia nell'anno precedente, in materia di cybersicurezza nazionale (art. 14, co. 1, D.L. n. 82/2021).

La disposizione specifica che tali dati rappresentano i dati ufficiali di riferimento degli attacchi informatici portati ai soggetti che operano nei settori rilevanti per gli interessi nazionali nel campo della cybersicurezza.

Da ultimo, si prevede che all'attuazione della disposizione si provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

La disposizione, inserita in prima lettura, è al momento sprovvista di **RT.**

Al riguardo, si rileva che le norme in esame prevedono per l'ACN nuovi compiti di raccolta, elaborazione e classificazione dei dati inerenti le notifiche degli incidenti informatici, nonché la loro esposizione nell'ambito della Relazione annuale da parte della medesima autorità: andrebbero pertanto fornite rassicurazioni in merito alla realizzabilità delle connesse procedure e trattamento dei dati avvalendosi delle sole risorse umane e strumentali già previste nei bilanci dell'Agenzia ai sensi della legislazione vigente.

Articolo 5
(Disposizioni in materia di Nucleo per la cybersicurezza)

L'articolo prevede la possibilità di far partecipare alle riunioni del Nucleo per la cybersicurezza ulteriori soggetti, quali rappresentanti della Direzione nazionale antimafia e antiterrorismo e rappresentanti della Banca d'Italia, in relazione a specifiche questioni di particolare rilevanza concernenti i compiti di proposta di iniziative in materia di cybersicurezza del Paese. Le amministrazioni e i soggetti convocati partecipano alle suddette riunioni a livello di vertice. A tal fine, si integra l'articolo 8 del decreto-legge 14 giugno 2021, n. 82.

La RT annessa al DDL iniziale (*ex* 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.

Al riguardo, per i profili di quantificazione, nel presupposto che l'allargamento della composizione e partecipazione alle riunioni del Nucleo non determini nuovi o maggiori oneri a carico dell'ACN, non ci sono osservazioni.

Articolo 6
(Disposizioni in materia di coordinamento operativo tra i servizi di informazione per la sicurezza e l'Agenzia per la cybersicurezza nazionale)

Il comma 1 prevede che, qualora i servizi di sicurezza della Repubblica, avuta notizia di un evento o di 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 attività di resilienza di competenza dell'Agenzia per la cybersicurezza nazionale, per il tramite del Dipartimento delle informazioni per la sicurezza ne informino il Presidente del Consiglio dei ministri o l'Autorità delegata per la sicurezza della Repubblica, ove istituita.

Il comma 2 dispone che, 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 la citata Agenzia, nonché il differimento di una o più delle sopra citate attività di resilienza.

La RT annessa al DDL iniziale evidenzia che l'articolo 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.

Al riguardo, convenendo con la RT in merito alla natura ordinamentale delle disposizioni in esame e alla loro neutralità, non ci sono osservazioni.

Articolo 7
(Composizione del Comitato interministeriale per la sicurezza della Repubblica)

L'articolo modifica la composizione del Comitato interministeriale per la sicurezza della Repubblica (CISR), disponendo che del Comitato facciano parte anche il Ministro dell'agricoltura, il Ministro delle infrastrutture e dei trasporti e il Ministro dell'università e della ricerca.

L'articolo, introdotto in prima lettura, è al momento sprovvisto di **RT**.

Al riguardo, per i profili di quantificazione, nulla da osservare.

Articolo 8
(Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza)

L'articolo, modificato in prima lettura, istituisce per le pubbliche amministrazioni indicate nell'articolo 1, comma 1 - laddove non sia già presente - la struttura preposta alle attività di cybersicurezza; al contempo, predispone l'istituzione del referente per la cybersicurezza, unico punto di contatto delle amministrazioni coinvolte con l'Agenzia per la cybersicurezza nazionale.

Il comma 1 individua, primariamente, i soggetti delle pubbliche amministrazioni coinvolti. Si tratta delle pubbliche amministrazioni trattate nell'articolo 1, comma 1, del disegno di legge salvo non presentino già la struttura costituenda. In particolare, si tratta di: le pubbliche amministrazioni centrali definite come tali dalla ricognizione annuale dell'ISTAT (art. 1, comma 3, legge n. 196 del 2009); le regioni e le province autonome di Trento e Bolzano; le città metropolitane; i comuni con una popolazione superiore ai 100.000 abitanti; i comuni capoluoghi di regione; le società di trasporto pubblico urbano con bacino di utenza non inferiore ai 100.000 abitanti; le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane; le aziende sanitarie locali; le società *in house* individuate all'articolo 1, comma 1.

Tali soggetti, qualora non la possiedano ancora, devono dotarsi di una struttura per la cybersicurezza, anche fra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente. In particolare tale struttura dovrà provvedere: allo sviluppo di politiche e procedure di sicurezza delle informazioni; alla produzione e l'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico; alla produzione e l'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione; alla produzione e aggiornamento di un piano programmatico per la sicurezza dei dati, sistemi e infrastrutture; la pianificazione e l'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza coi piani precedentemente elencati; alla pianificazione e l'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale; al monitoraggio e la valutazione continua delle minacce alla sicurezza e alla vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.

Il comma 2 istituisce la figura del soggetto referente per la cybersicurezza all'interno delle strutture appena descritte nel comma 1. Questo in particolare, viene individuato in ragione di specifiche professionalità e competenze possedute in materia. Nel caso in cui all'interno dei soggetti di cui all'articolo 1, comma 1, non vi siano dipendenti con tali requisiti potrà essere incaricato il dipendente di un'altra pubblica amministrazione previa autorizzazione da parte dell'amministrazione di appartenenza ai sensi dell'art. 53 del decreto legislativo n. 165 del 2001 e nell'ambito delle risorse disponibili a legislazione vigente. È stabilito che la citata figura svolga la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale in relazione a quanto previsto dalla legge e dalle normative settoriali in materia di cybersicurezza per le amministrazioni; il suo nominativo deve essere comunicato all'Agenzia per la cybersicurezza nazionale.

Il comma 3 prevede che la struttura per la cybersicurezza e il referente per la cybersicurezza istituiti dai commi 1 e 2 possano essere individuati nell'ufficio e nel responsabile per la transizione al digitale previsti dall'art. 17 del decreto legislativo n. 82 del 2005 (codice dell'amministrazione digitale).

Il comma 4 prevede che i compiti di cui ai commi 1 e 2 possono essere esercitati in forma associata, come previsto dall'articolo 17, commi 1-*sexies* e 1-*septies*, del C.A.D..

Il comma 5 attribuisce all'Agenzia per la cybersicurezza nazionale la possibilità di individuare le modalità e i processi di coordinamento e mutua collaborazione, anche di livello regionale, tra le amministrazioni di cui all'articolo 1, comma 1, e tra i referenti per la cybersicurezza al fine di facilitare la resilienza delle amministrazioni pubbliche.

Il comma 6 individua i soggetti e gli organi dello Stato a cui non si applicano le disposizioni del presente articolo. Nello specifico, la lettera a) precisa l'esclusione delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati inclusi nel perimetro di sicurezza nazionale cibernetica elencati all'interno del decreto del Presidente del Consiglio dei ministri n. 131 del 31 luglio 2020 (art. 1, co. 2-*bis*, decreto-legge n.105 del 2019). Per tali soggetti già risultano in vigore specifici obblighi di sicurezza. La lettera b) dispone l'esclusione per quegli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza (il Dipartimento delle informazioni per la sicurezza (DIS) (art. 4, legge n. 124 del 2007); l'Agenzia di informazione e sicurezza esterna (AISE) (art. 6, legge n. 124 del 2007); l'Agenzia di informazione e sicurezza interna (AISI) (art. 7, legge n. 124 del 2007)).

La RT annessa al DDL iniziale (*ex* articolo 6) conferma che l'articolo 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, 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 gli 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 gli 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.

Le modifiche ed integrazioni apportate all'articolo in esame sono al momento sprovviste di **RT.**

Al riguardo, occorre sottolineare che le norme in esame prevedono l'istituzione presso le PA di cui all'articolo 1, comma 1, della struttura e del referente per la cybersicurezza, avente le necessarie competenze tecniche, individuato quale punto unico di contatto con l'ACN, stabilendo che tale figura possa essere individuata anche nell'ufficio e nel responsabile per la transizione al digitale previsti dall'art. 17 del C.A.D. Le Amministrazioni interessate debbono provvedere nell'ambito delle sole risorse umane, strumentali e finanziarie disponibili a legislazione vigente e, ove non dispongano di tale personale, è prevista la possibilità di utilizzare un dipendente di altra amministrazione nell'ambito delle risorse disponibili, oppure di associarsi ad altre amministrazioni per l'impiego della medesima unità di personale.

Sul punto, andrebbero fornite maggiori informazioni circa i fabbisogni che comporta l'istituzione di tale struttura in relazione ai vari compiti di sviluppo, pianificazione, analisi e monitoraggio previsti dal comma 1. In relazione alle varie tipologie di amministrazioni pubbliche coinvolte andrebbero quindi fornite stime del personale e delle risorse necessarie, unitamente a informazioni sulle disponibilità che potranno essere destinate a tale struttura.

Posto che i commi 3 e 4 consentono l'individuazione della struttura e del referente nell'ufficio e nel responsabile per la transizione al digitale, già previsti dall'articolo 17 del d.lgs. n. 82/2005, rilevato che unificazione dei due uffici potrebbe consentire l'attuazione delle norme in esame realizzando economie, andrebbero forniti dati sull'effettiva istituzione dell'ufficio per la transizione digitale presso le pubbliche amministrazioni[1].

Inoltre, con riferimento alla figura del referente per la cybersicurezza, andrebbe valutata l'opportunità di chiarire nel testo del provvedimento quanto affermato dalla RT iniziale, ossia che al referente non spettano compensi aggiuntivi.

[1] Si ricorda che il recente decreto-legge n. 19/2024 (art. 20, comma 1, lett. a)), ha modificato la disciplina dell'ufficio per la transizione al digitale prevedendo modalità di aggregazione a livello regionale, potendo le amministrazioni territoriali avvalersi anche del supporto delle società *in house* mediante apposite convenzioni e senza aggravio per la finanza pubblica. La relativa relazione illustrativa ha affermato che tali modifiche sono previste "per l'effettiva strutturazione di tale ufficio e per potenziarne le funzioni".

Articolo 9
(Rafforzamento delle misure di sicurezza dei dati attraverso la crittografia)

L’articolo, introdotto nel corso dell’esame svoltosi in prima lettura, attribuisce alle strutture di cui all’articolo 8, preposte alle attività di cybersicurezza nelle pubbliche amministrazioni, la funzione di verificare che i programmi e le applicazioni informatiche e di comunicazione elettronica rispettino le linee guida sulla crittografia adottate dall'Agenzia per la cybersicurezza nazionale e dall'Autorità garante per la protezione dei dati personali e non contengano vulnerabilità note.

La medesima attività di verifica è attribuita alle strutture che svolgono analoghe funzioni per i soggetti rientranti nel perimetro di sicurezza cibernetica nazionale di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019 n. 105.

L’articolo, inserito nel corso dell’esame svoltosi in prima lettura, è al momento sprovvisto di **RT**.

Al riguardo, l’articolo reca la specificazione dei compiti delle strutture a presidio della cybersicurezza previste dall’articolo 8, da istituirsi presso le pubbliche amministrazioni, con funzione di verifica dei programmi e delle applicazioni informatiche e di comunicazione elettronica, in conformità con le linee guida sulla crittografia adottate dall'Agenzia per la cybersicurezza nazionale e dall'Autorità garante per la protezione dei dati personali al fine di escluderne fattori di vulnerabilità.

Per i profili interesse, si tratta di compiti che sembrerebbero richiedere la predisposizione di un sistema di vigilanza e monitoraggio/controllo costante sulle strutture informatiche delle PA interessate, con conseguente utilizzo delle risorse umane e strumentali necessarie a tal fine, sia per quanto concerne le strutture *hardware* che per gli applicativi *software*.

Si rinvia agli articoli 8 e 23.

Articolo 10
(Funzioni dell'Agenzia per la cybersicurezza nazionale in materia di crittografia)

L’articolo, interamente sostituito in prima lettura, valorizza l’utilizzo della crittografia quale strumento di difesa cibernetica e istituisce il Centro nazionale di crittografia presso l’Agenzia per la cybersicurezza nazionale – ACN. A tal fine viene novellato l'articolo 7, comma 1, del decreto-legge 14 giugno 2021, n. 82, prevedendo che l’ACN, anche attraverso una apposita sezione della strategia nazionale di cybersicurezza debba provvedere a:sviluppare e diffondere *standard*, linee guida e raccomandazioni al fine di rafforzare la cybersicurezza dei sistemi informatici; valutare la sicurezza dei sistemi crittografici; organizzare e gestire attività di divulgazione finalizzate a promuovere l'utilizzo della crittografia come strumento di cybersicurezza; promuovere, anche per il rafforzamento dell'autonomia industriale e tecnologica dell'Italia, la collaborazione con università e centri di ricerca per la valorizzazione dello sviluppo di nuovi algoritmi proprietari, la ricerca e il conseguimento di nuove capacità crittografiche nazionali nonché la collaborazione internazionale con gli organismi esteri che svolgono analoghe funzioni. A tal fine, la disposizione istituisce presso l'ACN 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. É previsto che il funzionamento del centro verrà disciplinato con apposito provvedimento del direttore generale dell'Agenzia. L’articolo in esame fa salve le competenze dell'Ufficio centrale per la segretezza.

La RT annessa al DDL iniziale (*ex* articolo 7), che fa riferimento ad un testo non più attuale, afferma che le 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.

La riformulazione è al momento sprovvista di **RT.**

Al riguardo, considerato che la disposizione in esame prevede il potenziamento delle funzioni dell'Agenzia in materia di crittografia e l'istituzione, presso la stessa Agenzia, del Centro nazionale di crittografia, andrebbe dimostrata l'effettiva possibilità di istituire tale nuovo soggetto ad invarianza d'oneri.

Tali norme appaiono infatti suscettibili di riflettersi in fabbisogni aggiuntivi di risorse umane e strumentali a carico dell'Agenzia, di cui andrebbero fornite stime evidenziando le risorse disponibili a tal fine.

Articolo 11
(Procedimento amministrativo sanzionatorio per l'accertamento e la contestazione delle violazioni in materia di cybersicurezza di competenza dell'Agenzia per la cybersicurezza nazionale)

L'articolo definisce termini e modalità per l'adozione del regolamento che stabilisce i criteri, anche temporali, per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia. Prevede che nelle more dell'adozione del regolamento, trovi applicazione il capo I, sezioni I e II, della legge sulle sanzioni amministrative (legge n. 689/1981).

La RT annessa al DDL iniziale (*ex* articolo 8), dopo aver illustrato la disposizione, afferma che non comporta 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 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.

Al riguardo, per i profili di quantificazione, in relazione alle entrate da sanzioni si segnala che i relativi incassi sono riassegnati in conto entrate all'Agenzia per la cybersicurezza nazionale di cui all'articolo 11, comma 2, lettera *f*), del decreto-legge n. 82 del 2021. Al riguardo, non si hanno osservazioni da formulare, atteso che il riversamento di tali introiti all'Agenzia è già previsto dalla normativa vigente.

Articolo 12
(Disposizioni in materia di personale dell'Agenzia per la cybersicurezza nazionale)

Il comma 1, introducendo il nuovo comma 8-*ter* all'articolo 12 del decreto-legge 14 giugno 2021, n. 82, stabilisce un divieto, della durata di due anni, di assunzione di altri incarichi, presso soggetti privati, finalizzati allo svolgimento di mansioni in materia di cybersicurezza, nei confronti di dipendenti appartenenti al ruolo del personale dell'Agenzia per la cybersicurezza nazionale – ACN che abbiano partecipato, nell'interesse e a spese dell'Agenzia stessa, a specifici percorsi formativi di specializzazione. Sono tuttavia previste specifiche cause di esclusione dall'applicazione del richiamato divieto.

Il comma 2 prevede che fino al 2026 per il personale dell'Agenza della cybersicurezza il requisito della permanenza minima nell'Area operativa per il passaggio all'Area manageriale e alte professionalità è fissato in tre anni.

La RT annessa al DDL iniziale (*ex* articolo 9) conferma che la disposizione 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 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.

Il comma 2 è al momento sprovvisto di **RT**.

Al riguardo, sul comma 1, in considerazione del tenore ordinamentale delle disposizioni, si conviene con la RT circa l'assenza di nuovi o maggiori oneri per la finanza pubblica.

Sul comma 2, andrebbe chiarito se il termine posto dalla norma potrebbe determinare un'accelerazione nel passaggio dalla carriera amministrativa a quella manageriale nell'Agenzia, indicando le differenze retributive tra le due aree, la platea che potrebbe essere interessata dalla norma e le risorse che potranno essere utilizzate per eventuali incrementi retributivi[2].

Ciò, anche considerando che al personale dell'Autorità in parola, quanto agli avanzamenti interni tra segmenti professionali, così come per la progressione economica

[2] Sul punto, va segnalato che il bilancio di previsione (*budget economico*) dell'ACN per il 2023 (ultimo disponibile) evidenziava l'assenza di avanzo di esercizio per il medesimo anno. Cfr. Agenzia per la cybersicurezza nazionale (ACN), Deliberazione del Direttore generale del 31 ottobre 2022, Allegati, pagina 13, approvato con DPCM 19 dicembre 2022.

prevista nell'ambito delle varie categorie, dovrebbe applicarsi una disciplina analoga quella prevista per il personale della Banca d'Italia, ovvero per "merito comparato", a scelta, del Direttore generale[3].

Articolo 13
(Disposizioni in materia di personale degli organismi di informazione e sicurezza)

L'articolo, inserito nel corso dell'esame svoltosi in prima lettura, introduce ai commi 1- 5 alcune disposizioni in materia di personale del sistema di informazione per la sicurezza della Repubblica.

In particolare, al comma 1 si dispone che coloro abbiano ricoperto la carica di direttore generale e di vice direttore generale del Dipartimento delle informazioni per la sicurezza (DIS), dell'Agenzia informazioni e sicurezza esterna (AISE) o dell'Agenzia informazioni e sicurezza interna (AISI), ovvero vi abbiano svolto incarichi dirigenziali di prima fascia di preposizione a strutture organizzative di livello dirigenziale generale, non possano nei tre anni successivi alla cessazione dell'incarico svolgere – salvo autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità delegata ove istituita – attività lavorativa, professionale o consulenziale, né possano ricoprire cariche, presso soggetti esteri, pubblici o privati, ovvero presso soggetti privati italiani che svolgano attività di rilevanza strategica (secondo la perimetrazione resa dal decreto-legge n. 21 del 2012). L'autorizzazione allo svolgimento dell'attività lavorativa o di cariche è concessa avuto comunque riguardo alle esigenze di protezione del patrimonio informativo acquisito e di evitare pregiudizi per la sicurezza nazionale.

Il comma 2 pone un divieto – inderogabile – al personale del ruolo unico del personale dei servizi di informazione per la sicurezza e del DIS di svolgere, nei tre anni successivi alla cessazione dal servizio, attività lavorativa, professionale o consulenziale, ovvero ricoprire cariche, presso enti o privati titolari di licenza per prestare vigilanza o custodia, o comunque presso soggetti che a qualunque titolo svolgano attività di investigazione, ricerca o raccolta informativa.

Il comma 3 prevede per il medesimo personale, qualora abbia partecipato a specifici percorsi formativi di specializzazione nell'interesse e a spese delle DIS, dell'AISE e dell'AISI, un divieto di assunzione o di assunzione di incarichi presso soggetti privati, per svolgere le mansioni per le quali abbia beneficiato delle attività formative medesime. Il divieto ha la durata di tre anni a decorrere dalla data di completamento dell'ultimo dei percorsi formativi.

Il comma 4 stabilisce che i contratti stipulati e gli incarichi conferiti in violazione dei divieti di cui al presente articolo sono nulli.

Il comma 5 demanda a regolamento adottato con apposito d.P.C.m previo parere del Comitato parlamentare per la sicurezza della Repubblica e sentito il Comitato interministeriale per la sicurezza

---

[3] Sul punto, si segnala che il Regolamento del personale dell'Agenzia di cui al DPCM n. 224 del 2021 stabilisce al comma 1 dell'articolo 54 che il sistema di avanzamento del personale si articola in passaggi di segmento professionale e di "livello economico". L'articolo 3 del medesimo regolamento prevede che nell'Area "operativa" sono previsti i seguenti segmenti professionali: a) Coordinatore *(Supervisor*); b) Assistente (*Assistant*). Il comma 3 dell'articolo 57 prevede che per il passaggio di "segmento professionale" anche ad Esperto/Consigliere (carriera manageriale) si provveda mediante la verifica, nei confronti di coloro i quali avanzino la propria candidatura, da parte del Comitato di cui all'articolo 58, comma 2, del Regolamento, secondo criteri omogenei per l'intera Agenzia, predeterminati dal Direttore generale e comunicati agli interessati, valutando i singoli in comparazione con gli altri elementi inquadrati nel segmento. In particolare, è stabilito che la verifica sia effettuata comunque sulla base: a) della storia professionale maturata nel segmento di provenienza; b) del possesso delle caratteristiche necessarie per l'esercizio dei ruoli manageriali/professionali propri del segmento professionale superiore. I dati aggiornati al 31 dicembre 2023 indicano 213 unità complessive in servizio, di cui 130 unità nell'Area manageriale/Alte professionalità,11 unità dell'Area operativa e 72 unità con contratto a t.d. La specialità dell'ordinamento del personale e degli organici dell'Agenzia è modulata secondo i criteri stabiliti dall'articolo 12 del decreto-legge n. 82/2021. Cfr. ACN, "Amministrazione trasparente", sito *internet*, dati inerenti al personale presente.

.

della Repubblica la definizione delle procedure di autorizzazione – per i casi autorizzabili, ai sensi del comma 1 – nonché gli obblighi di dichiarazione e di comunicazione a carico dei dipendenti.

L'integrazione è al momento sprovvista di **RT.**

Al riguardo, per i profili di quantificazione, ritenuto il carattere ordinamentale delle disposizioni in esame, i cui effetti appaiono iscriversi appieno nell'ambito di quelli già contemplati dai tendenziali di spesa a legislazione vigente, non ci sono osservazioni.

Articolo 14
(Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e disposizioni di raccordo con il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133)

Il comma 1 prevede l'adozione di un 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 e previo parere del Comitato interministeriale per la sicurezza della Repubblica (CISR), al fine di individuare, per determinate categorie tecnologiche di beni e servizi informatici, 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. Si precisa, inoltre, che per elementi essenziali di cybersicurezza si intende "l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela" degli interessi nazionali strategici. A seguito dell'approvazione di una modifica in prima lettura, il DPCM individua 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 italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi tra quelli che sono parte di accordi di collaborazione con l'UE e o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione. I soggetti tenuti a rispettare tali elementi essenziali nell'acquisto di beni ICT sono quelli indicati nell'articolo 2, comma 2, del codice dell'amministrazione digitale (D.Lgs. 82/2005), ossia: le pubbliche amministrazioni, comprese le autorità di sistema portuale e le autorità amministrative indipendenti di garanzia, vigilanza e regolazione; i gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse; le società a controllo pubblico, escluse le società quotate a meno che non gestiscano servizi di pubblico interesse.

Il comma 2 prevede, nell'ambito dei contratti di approvvigionamento di beni e servizi informatici di cui al comma 1, una serie di obblighi e facoltà in capo alle stazioni appaltanti, incluse le centrali di committenza, in relazione agli elementi essenziali di cybersicurezza individuati dal comma precedente. Nel dettaglio viene previsto che le stazioni appaltanti: possono esercitare la facoltà di non aggiudicare il contratto di cui agli articoli 107, comma 2, e 108, comma 10, del D.Lgs. 36/2023 (Codice dei contratti pubblici), se accertano che l'offerta non tiene conto degli elementi essenziali di cybersicurezza; considerano sempre 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; nel caso in cui sia utilizzato il criterio del minor prezzo, ai sensi dell'articolo 108, comma 3, del Codice dei contratti pubblici, inseriscono gli elementi di cybersicurezza di cui al comma 1 tra i requisiti minimi dell'offerta; nel caso in cui sia utilizzato il criterio dell'offerta economicamente più vantaggiosa, 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%; prevedono – nei casi individuati dal DPCM di cui al comma 1 - criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti alla NATO o Paesi terzi individuati con DPCM.

Il comma 3 prevede che rientrano nel campo di applicazione della disposizione di cui sopra anche i soggetti privati, non compresi tra quelli di cui sopra, ma rientranti nel perimetro di sicurezza nazionale cibernetica (PSNC) di cui all'articolo 1, comma 2-*bis*, del D.L. n. 105/2019. Si tratta dei soggetti aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

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

La RT annessa al DDL iniziale segnala che la norma 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 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.

Al riguardo, per i profili di quantificazione, ritenuto il carattere ordinamentale delle disposizioni in esame, non ci sono osservazioni.

Articolo 15
(Modifica all'articolo 16 della legge 21 febbraio 2024, n.15)

L'articolo, inserito in prima lettura[4], individua 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. A tal fine, all'articolo 16, comma 2, della legge 21 febbraio 2024, n.

[4] Cfr. Camera dei deputati, Bollettino delle Giunte e delle Commissioni parlamentari, 8 maggio 2024, pagina 29.

15, dopo la lettera c) è inserita lettera c-*bis*), che prevede che il Governo sarà tenuto ad apportare alla disciplina degli intermediari finanziari iscritti nell'albo previsto dall'articolo 106 del decreto legislativo 1° settembre 1993, n. 385 e di Poste italiane SpA per l'attività del patrimonio Bancoposta (di cui al decreto del Presidente della Repubblica 14 marzo 2001, n. 144), le occorrenti modifiche e integrazioni, anche mediante la normativa secondaria di cui alla lettera d) del medesimo articolo 16, per conseguire un livello elevato di resilienza operativa digitale e assicurare la stabilità del settore finanziario nel suo complesso, in particolare: i) definendo presidi in materia di resilienza operativa digitale equivalenti a quelli stabiliti nel regolamento (UE) 2022/2554; ii) tenendo conto, nella definizione dei presidi di cui al punto i), del principio di proporzionalità e delle attività svolte dagli intermediari finanziari e da Bancoposta; iii)attribuendo alla Banca d'Italia l'esercizio nei confronti di questi soggetti dei poteri di vigilanza, di indagine e sanzionatori richiamati alla lettera b) del medesimo articolo 16.

L'integrazione è al momento sprovvista di **RT**.

Al riguardo, per i profili di quantificazione, non ci sono osservazioni.

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

Articolo 16
(Modifiche al codice penale)

L'articolo reca modifiche al codice penale in materia di prevenzione e contrasto dei reati informatici.

Il comma 1, lettera a), reca disposizioni conseguenti alle modifiche introdotte dalla successiva lettera t) (vedi infra).

Alla lettera b), si modifica l'art. 615-*ter* c.p. (*Accesso abusivo a un sistema informatico o telematico*). Le modifiche introdotte sono volte ad ampliare l'ambito di applicazione della fattispecie e a inasprire il trattamento sanzionatorio elevando le pene previste.

La lettera c) modifica l'art. 615-*quater* c.p. (*Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici*). La disposizione in commento modifica, in primo luogo, la definizione della fattispecie delittuosa, ampliando il dolo specifico previsto per la configurabilità della fattispecie operando la sostituzione della nozione di "profitto" prevista dal testo vigente con quella, più ampia, di "vantaggio" (n. 1). Inoltre, vengono ridefinite le aggravanti.

Con la lettera d) è abrogato l'articolo 615-*quinquies (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)*;

Con la lettera e), si interviene sull'art. 617-*bis* c.p. (*Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche e telefoniche*). La disposizione inserisce un ulteriore comma volto a prevedere una circostanza aggravante, con l'applicazione della reclusione da 2 a 6 anni, qualora ricorra taluna delle circostanze di cui all'art. 615-*ter*, secondo comma, n. 1, vale a dire la commissione del fatto da parte di un pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri, da un investigatore privato anche abusivo, o con abuso della qualità di operatore di sistema.

La lettera f) interviene sull'art. 617-*quater* c.p. (*Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*). La disposizione in commento reca, in primo luogo, alcune modifiche al quarto comma in materia di circostanze aggravanti, concernenti: l'innalzamento della pena prevista per le fattispecie aggravate, con la previsione della reclusione da 4 a 10 anni (anziché da 3 a 8 anni) (n. 1); la previsione dell'aggravante della commissione del fatto su 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 previsione dell'aggravante della commissione del fatto in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni.

La lettera g) interviene sull'art. 617-*quinquies* c.p. (*Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche*). La disposizione in commento reca modifiche alla disciplina delle aggravanti, innalzando le pene e ridefinendo le fattispecie, analogamente a quanto previsto dalla lett. f) per l'art. 617-*quater*.

La lettera h) interviene sull'art. 617-*sexies* c.p. (*Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*). La disposizione in commento innalza la pena per la fattispecie aggravata, per la quale si prevede la reclusione da 3 a 8 anni (anziché da 1 a 5 anni)

La lettera i) reca una disposizione di coordinamento volta a modificare la rubrica del capo III-*bis* del titolo XII del libro secondo del codice penale, ora denominata "*Disposizioni comuni*", conseguentemente all'introduzione dell'art. 623-*quater*.

La lettera l) prevede l'inserimento nel codice penale dell'art. 623-*quater* in materia di circostanze attenuanti per i delitti di cui agli artt. 615-*ter* (*Accesso abusivo a un sistema informatico o telematico*), 615-*quater* (*Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici*), 617-*quater* (*Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*), 617-*quinquies* (*Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche*) e 617-*sexies* (*Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*) del codice penale. Sono previste: una circostanza attenuante a effetto comune (diminuzione della pena fino a un terzo) quando il fatto sia di lieve entità, avuto riguardo alla natura, alla specie, ai mezzi, alle modalità o alle circostanze dell'azione o alla particolare tenuità del danno o del pericolo (primo comma del nuovo art. 623-*quater*); una circostanza attenuante a effetto speciale (diminuzione della pena dalla metà a due terzi) in favore di chi si adopera per evitare che l'attività delittuosa sia portata a ulteriori conseguenze, anche aiutando concretamente l'autorità giudiziaria o l'autorità di polizia nella raccolta di prove o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi (secondo comma del nuovo art. 623-*quater*). Alle predette attenuanti non si applica il divieto di prevalenza sancito dall'art. 69, quarto comma, c.p. (terzo comma del nuovo art. 623-*quater).*

La lettera m) aggiunge un comma all'art. 629 c.p. (*Estorsione*) che prevede la fattispecie del delitto di estorsione mediante reati informatici, realizzata dalla costrizione di taluno a fare o ad omettere qualche cosa, procurando a sé o ad altro un ingiusto profitto, mediante le condotte, o la minaccia di compierle, di cui reati indicati. Si prevede che la nuova fattispecie delittuosa sia punita con la reclusione da 6 a 12 anni e con la multa da euro 5.000 a euro 10.000. Si prevede la reclusione da 8 a 22 anni e la multa da euro 6.000 a euro 18.000 se ricorre taluna delle circostanze indicate nell'ultimo capoverso dell'articolo precedente.

La lettera n) interviene sull'art. 635-*bis* c.p. (*Danneggiamento di informazioni, dati e programmi informatici*). La disposizione prevede:· l'innalzamento della pena per la fattispecie semplice, prevedendo la reclusione da 2 a 6 anni (anziché da 6 mesi a 3 anni); l'ampliamento della fattispecie aggravata, prevedendo che essa ricorra se il fatto è commesso: da parte di un pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri, da un investigatore privato anche abusivo; usando violenza o minaccia o da parte di persona palesemente armata; l'innalzamento della pena per la fattispecie aggravata, prevedendo la reclusione da 3 a 8 anni (anziché da 1 a 4 anni).

La lettera o) interviene sull'art. 635-*ter* c.p. (*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*), in particolare sulla definizione della fattispecie delittuosa e sulle circostanze aggravanti.

La lettera p) interviene sull'art. 635-*quater* c.p.p. (*Danneggiamento di sistemi informatici o telematici)* e prevede (con modifiche analoghe a quelle previste per l'art. 635-*bis*, vedi sopra): l'innalzamento della pena per la fattispecie semplice, con la reclusione da 2 a 6 anni (anziché da 1 a 5 anni); l'ampliamento della fattispecie aggravata; la ridefinizione della pena per la fattispecie aggravata, con la reclusione da 3 a 8 anni (anziché l'aumento fino a un terzo previsto dal testo vigente).

La lettera q) introduce nel codice penale l'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*). Il primo comma del nuovo articolo riproduce il vigente art. 615-*quinquies* c.p.10 (che viene contestualmente abrogato dalla lett. *d*): è punito con la reclusione fino a 2 anni e con la multa fino a euro 10.329 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. Il secondo e il terzo comma prevedono le circostanze aggravanti.

La lettera r) sostituisce l'art. 635-*quinquies* c.p. (*Danneggiamento di sistemi informatici o telematici di pubblica utilità*): rispetto al testo vigente si prevede l'innalzamento della pena e la sostituzione della nozione di servizi informatici o telematici di pubblica utilità con quella di servizi informatici o telematici di pubblico interesse. Quanto alle modalità della condotta la disciplina vigente non è sostanzialmente innovata. Il secondo comma disciplina le circostanze aggravanti. Il terzo comma prevede, nel caso di concorso di taluna delle circostanze la pena della reclusione da 4 a 12 anni.

La lettera s) prevede l'inserimento nel codice penale dell'art. 639-*ter* in materia di circostanze attenuanti per i delitti di cui agli artt. del codice penale 629, terzo comma, introdotto dalle lett. l) (*Estorsione mediante reati informatici*, vedi sopra), 635-*ter* (*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*), 635-*quater*.1 (*Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*) e 635-*quinquies*, modificato alla lett. q) (*Danneggiamento di sistemi informatici o telematici di pubblico interesse*). Sono previste: una circostanza attenuante a effetto comune (diminuzione della pena fino a un terzo) quando il fatto sia di lieve entità, avuto riguardo alla natura, alla specie, ai mezzi, alle modalità o alle circostanze dell'azione o alla particolare tenuità del danno o del pericolo (primo comma del nuovo art. 639-*ter*); una circostanza attenuante a effetto speciale (diminuzione della pena dalla metà a due terzi) in favore di chi si adopera per evitare che l'attività delittuosa sia portata a ulteriori conseguenze, anche aiutando concretamente l'autorità giudiziaria o l'autorità di polizia nella raccolta di prove o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi (secondo comma del nuovo art. 639-*quater*). Alle predette attenuanti non si applica il divieto di prevalenza sancito dall'art. 69, quarto comma, c.p. (terzo comma del nuovo art. 639-*quater*).

La lettera t) inserisce nell'art. 640 c.p., secondo comma, una nuova circostanza aggravante del reato di truffa (numero 2-*ter*), nel caso in cui il fatto sia commesso a distanza attraverso strumenti informatici o telematici idonei ad ostacolare la propria o altrui individuazione. La medesima lettera t), inoltre, prevede l'applicazione alla nuova circostanza aggravante del reato di truffa del regime di procedibilità a querela della persona offesa, diversamente da quanto disposto per le altre fattispecie aggravate del reato di truffa che sono invece procedibili d'ufficio.

Consequenziali al suddetto intervento sono le modifiche apportate dalle lettere a) e u), che intervengono, rispettivamente, sugli articoli 240 c.p. e 640-*quater* c.p. per disporre, in relazione al reato di truffa aggravata introdotto dalla lettera t): la misura di sicurezza prevista dall'art. 240, comma 2, c.p. che disciplina la confisca obbligatoria dei beni e degli strumenti informatici o telematici utilizzati in

tutto o in parte per la commissione del reato, nonché dei beni che costituiscono il profitto o il prodotto del reato medesimo ovvero di somme di denaro, beni o altre utilità di cui il colpevole ha la disponibilità per un valore corrispondente a tale profitto o prodotto, se non è possibile eseguire la confisca diretta del profitto o del prodotto; l'osservanza, in quanto applicabili, delle disposizioni contenute nell'art. 322-*ter* c.p., che stabilisce, in caso di condanna o di applicazione della pena su richiesta delle parti, la confisca dei beni che costituiscono il profitto o il prezzo del reato, salvo che appartengano a persona estranea al reato, ovvero, quando essa non è possibile, la confisca di beni, di cui il reo ha la disponibilità, per un valore corrispondente a tale prezzo o profitto.

La RT annessa al DDL iniziale (*ex* articolo 11), dopo aver descritto le norme, evidenzia che dal punto di vista finanziario le modifiche introdotte al codice penale hanno carattere ordinamentale e precettivo e non sono suscettibili di determinare nuovi o maggiori oneri a carico della finanza pubblica.

Il prospetto riepilogativo degli effetti d'impatto attesi sui saldi di finanza pubblica non espone valori.

Al riguardo, si rileva che le disposizioni ampliano l'ambito di applicazione di alcune fattispecie disciplinate dal codice penale e inaspriscono il trattamento sanzionatorio previsto con riferimento ai reati informatici o perpetrati con mezzi informatici.

Per i profili di quantificazione, si conviene con la RT in merito al tenore essenzialmente ordinamentale e precettivo delle disposizioni, non suscettibile pertanto di determinare nuovi o maggiori oneri di spesa.

Articolo 17
(Modifiche al codice di procedura penale)

L'articolo reca modifiche al codice di procedura penale finalizzate a recepire gli interventi in materia di prevenzione e contrasto dei reati informatici introdotte dal precedente articolo 16. Per tali reati si prevedono: l'attribuzione della competenza sulle indagini alla procura distrettuale; la deroga al regime ordinario per la proroga delle indagini preliminari; termini di durata massima delle indagini preliminari pari a 2 anni.

La RT annessa al DDL iniziale (ex articolo 12), dopo aver descritto le norme, evidenzia che le modifiche introdotte al codice di procedura penale 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.

Il prospetto riepilogativo degli effetti d'impatto attesi sui saldi di finanza pubblica non espone valori.

Al riguardo, ritenuto il tenore ordinamentale delle norme, nulla da osservare.

Articolo 18
(Modifiche alle norme sui collaboratori di giustizia di cui al decreto-legge n. 8 del 1991)

L'articolo reca alcune modifiche alle disposizioni relative ai soggetti che collaborano con la giustizia, di cui al decreto-legge n. 8 del 1991, volte ad estendere il campo di applicazione della relativa disciplina agli autori dei reati informatici di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale.

La RT annessa al DDL iniziale (*ex* articolo 13) conferma che le disposizioni introducono modifiche al D.L. n. 8/1991, convertito, con modificazioni, dalla L. n. 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 competenti 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.

Durante l'esame in prima lettura, il Governo ha precisato che "dal 2017 ad oggi, si è registrato un calo del numero dei collaboratori ammessi a programma a fronte dell'invarianza delle risorse assegnate sui capitoli di bilancio interessati". In tal senso ha assicurato la capienza delle risorse iscritte in bilancio a legislazione vigente a fronte delle esigenze finanziarie derivanti dall'estensione del campo di applicazione delle disposizioni di protezione dei soggetti che collaborano con la giustizia anche agli autori dei reati informatici più gravi[5].

Al riguardo, prendendo atto delle risposte fornite in prima lettura, sarebbe comunque utile disporre dei dati sulle risorse iscritte in bilancio a legislazione vigente, sul loro utilizzo e sulla quota che potrebbe essere utilizzata per far fronte alle esigenze finanziarie derivanti dall'estensione del campo di applicazione delle disposizioni di protezione dei soggetti che collaborano con la giustizia anche agli autori dei reati informatici più gravi.

---

[5] Cfr. Ministero dell'economia e delle finanze, Appunto dell'Ufficio del coordinamento legislativo, in Camera dei deputati, Bollettino delle Giunte e delle Commissioni parlamentari, 14 maggio 2024, pagina 45.

Articolo 19
(Modifica al decreto-legge 13 maggio 1991, n. 152, in materia di intercettazioni)

L’articolo estende la disciplina delle intercettazioni prevista per i fatti di criminalità organizzata ai reati informatici rimessi al coordinamento del procuratore nazionale antimafia e antiterrorismo. In queste ipotesi, l'autorizzazione all’intercettazione è soggetta a limiti meno stringenti, potendo essere concessa:

- quando sussistono "sufficienti indizi" di reato (anziché gravi indizi);
- quando è "necessaria per lo svolgimento delle indagini" (anziché assolutamente indispensabile).

La RT annessa al DDL iniziale (*ex* articolo 14), dopo aver descritto la norma, afferma che la sua 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.

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.

Durante l’esame in prima lettura, il Governo ha aggiunto che “i recenti interventi, volti alla razionalizzazione e al contenimento delle tariffe sia delle prestazioni obbligatorie che di quelle funzionali alle operazioni di intercettazione, determineranno gradualmente, congrui risparmi di spesa in relazione alla materia esaminata. Si fa riferimento, in particolare, all'attuazione del decreto del Ministro della giustizia 6 ottobre 2022, di concerto con il Ministro dell'Economia e delle Finanze recante "Disposizioni per l'individuazione delle prestazioni funzionali alle operazioni di intercettazioni e per la determinazione delle tariffe ai sensi dell'articolo 1, comma 89, della legge 23 giugno 2017, n. 103". E' stato infatti ipotizzato che l'applicazione del nuovo listino, contenente anche significative riduzioni delle tariffe in caso di noleggi con durata prolungata nel tempo, comporterà risparmi di spesa come richiesto dal

legislatore, assicurando il livello qualitativo dei servizi resi in favore dell'autorità giudiziaria (che devono sempre essere al passo dell'evoluzione tecnologica che contraddistingue il settore) e tenendo conto della rilevanza della materia nel rispetto delle dinamiche a cui gli operatori del mercato sono soggetti. Tuttavia, il valore delle liquidazioni effettuate nell'anno 2023 ha tenuto conto solo in parte delle nuove tariffe, poiché il nuovo listino si è applicato alle attività avviate successivamente al 15 dicembre 2022, non dispiegando allo stato gli effetti di risparmio previsti. Si evidenzia altresì che sulla spesa in questione incide il frequente ricorso alle intercettazioni con nuove tecnologie, il cui uso è rimesso all'esclusiva valutazione dell'autorità giudiziaria sul cui potere discrezionale di indagine questa amministrazione non ha alcuna facoltà di intervenire.". Per quanto esposto, il Ministero dell'economia e delle finanze ha quindi concluso che "le esigenze finanziarie derivanti dall'eventuale maggior numero di intercettazioni, potranno essere sostenute attraverso una riprogrammazione delle risorse che verranno rese disponibili dai citati risparmi di spesa" [6].

Al riguardo, considerando le informazioni contenute nella RT in merito alle risorse già previste ai sensi della legislazione vigente e gli elementi acquisiti nel corso dell'esame in prima lettura, si rileva anzitutto che le risposte fornite non assicurano con certezza circa l'esistenza di risparmi e che l'entità della spesa dipende anche da fattori non controllabili dall'amministrazione, quali le decisioni dell'autorità giudiziaria. In prima approssimazione sarebbe pertanto utile disporre del dato della spesa attuale per intercettazioni riguardante i reati informatici, a cui poter applicare un fattore di incremento per effetto dei requisiti meno stringenti ora previsti e delle nuove fattispecie penali introdotte all'articolo 16, al fine di determinare sommariamente l'entità della nuova spesa.

Si ricorda che la spesa per intercettazioni, appostata al capitolo 1363 dello stato di previsione del Ministero della giustizia, si qualifica come spesa di natura giuridicamente obbligatoria [7], per cui è consentito il prelievo dal fondo di riserva per spese obbligatorie.

Articolo 20
(Modifiche al decreto legislativo 8 giugno 2001, n. 231)

L'articolo interviene sul catalogo dei reati presupposto della responsabilità amministrativa degli enti, contemplato dall'articolo 24-*bis* del decreto legislativo n. 231 del 2001.

In particolare:

---

6 Cfr. Ministero dell'economia e delle finanze, Appunto dell'Ufficio del coordinamento legislativo, in Camera dei deputati, Bollettino delle Giunte e delle Commissioni parlamentari, 14 maggio 2024, pagine 45-46.

7 Si ricorda che il capitolo 1363 è incluso nell'elenco 1, allegato allo stato di previsione della spesa del Ministero dell'economia e delle finanze, recante l'elenco dei capitoli/piani gestionali per i quali è concessa la facoltà di prelevamento dal fondo di riserva per le spese obbligatorie. Come risulta dal rendiconto per l'anno 2022 (ultimo rendiconto al momento disponibile), lo stanziamento iniziale in termini di competenza del citato capitolo era pari a 213.718.734 euro e che esso, per effetto di un incremento disposto nel corso dell'esercizio con provvedimento amministrativo (DMC n. 34613 del 2022), per un ammontare pari a 6.300.000 euro, era stato elevato a 220.018.734 euro, impegnati pressoché integralmente al termine dell'esercizio stesso.

- si aumentano le 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;
- si introduce nell'articolo 24-*bis* il nuovo comma 1-*bis*, ai sensi del quale si applica all'ente la sanzione pecuniaria da trecento a ottocento quote in relazione alla commissione della nuova fattispecie di estorsione informatica di cui all'articolo 629, terzo comma, del codice penale;
- si modifica il comma 2 dell'articolo 24-*bis*, elevando la sanzione pecuniaria ivi prevista sino a quattrocento quote (attualmente è "fino a trecento quote") e sostituendo tra i reati presupposti per i quali è prevista l'applicazione all'ente della sanzione pecuniaria suddetta il riferimento all'articolo 615-*quinquies* c.p. (abrogato dall'articolo 16, lettera d) del presente ddl) con il richiamo al nuovo delitto 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 635-*quater*.1;
- si integra il comma 4, laddove dopo il primo periodo è inserita una disposizione per cui 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.

La RT annessa al DDL iniziale (ex articolo 15) conferma che la norma apporta modificazioni all'articolo 24-*bis* del decreto legislativo 8 giugno 2001, n. 231 in materia di delitti informatici e trattamento illecito dati.

Dopo averne descritto il contenuto, afferma che 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.

Al riguardo, premesso che le norme in esame inaspriscono le sanzioni a cui sono assoggettati gli enti qualora reputati amministrativamente responsabili di delitti informatici o del trattamento illecito di dati, ritenuto il carattere ordinamentale delle disposizioni e il fatto che non vengono scontati effetti finanziari positivi derivanti dall'incremento delle sanzioni, nulla da osservare.

Articolo 21
(Modifica alla legge 11 gennaio 2018, n. 6)

L'articolo interviene sul procedimento di applicazione delle speciali misure di protezione per i testimoni di giustizia e per gli altri protetti, prevedendo che la Commissione centrale debba richiedere il parere al Procuratore nazionale antimafia e antiterrorismo sulla proposta di ammissione alle speciali misure, anche nel caso dei gravi delitti informatici indicati nell'articolo 371-*bis*, comma 4--*bis*, c.p.p.. A tal fine, si modifica il comma 2 dell'articolo 11 della legge 11 gennaio 2018, n. 6.

La RT annessa al DDL iniziale (*ex* articolo 16) evidenzia che la norma apporta modifiche alla legge 11 gennaio 2018, n. 6, ed in particolare al 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.

Al riguardo, convenendo con la RT circa il tenore ordinamentale e procedurale della norma, nulla da osservare.

Articolo 22
(Modifiche al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109)

L'articolo, al comma 1, lettere a) e b), disciplina i rapporti tra l'Agenzia per la cybersicurezza nazionale (ACN), il procuratore nazionale antimafia e antiterrorismo, la polizia giudiziaria ed il pubblico ministero

In particolare, la lettera a) modifica il comma 4 dell'articolo 17 del decreto-legge n. 82 del 2021, prevedendo che la trasmissione delle notifiche di incidente 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 n. 144 del 2005, debba essere immediata. È confermato il riconoscimento al personale dell'Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni, della qualifica di pubblico ufficiale. La trasmissione delle notifiche di incidente, che rientra tra i compiti del CSIRT, rimane inquadrata tra gli obblighi di denuncia fissati dall'articolo 331 del codice di procedura penale, concernente appunto la denuncia da parte di pubblici ufficiali e incaricati di un pubblico servizio.

La lettera b) introduce poi nell'articolo 17 del decreto-legge n. 82 del 2021 quattro ulteriori commi (commi da 4-*bis*.1 a 4-*bis*.4). Ai sensi del nuovo comma 4-*bis*.1 l'Agenzia deve procedere alle attività di cui all'articolo 7, comma 1, lett. n) (sviluppo di capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici) e n-*bis*) (analisi e supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi) e informare senza ritardo il procuratore nazionale antimafia e antiterrorismo nei casi in cui ha notizia di un attacco ai sistemi informatici o telematici di cui all'articolo 371-*bis*, comma 4-*bis* c.p.p., e, in ogni caso quando risulti interessato taluno dei soggetti rientranti nel Perimetro di sicurezza nazionale, degli operatori di servizi essenziali e dei fornitori di servizio digitale, delle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico. Corrispondentemente il PM – quando acquisisce la notizia dei gravi delitti informatici indicati nell'articolo 371-*bis*, comma 4-*bis* c.p.p.– deve darne tempestiva informazione all'ACN assicurando anche il raccordo informativo con l'organo del Ministero dell'interno per la sicurezza e la regolarità dei

servizi di telecomunicazione. Il PM, in ogni caso, ricevuta la notizia di reato e assunta la direzione delle indagini, è chiamato ad impartire le disposizioni necessarie ad assicurare che gli accertamenti urgenti si svolgano tenendo conto delle attività di ripristino svolte dall'Agenzia e può eventualmente disporre il differimento di una o più delle attività, con motivato provvedimento adottato senza ritardo, per evitare un grave pregiudizio per il corso delle indagini (comma 4-*bis*.3 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).

La RT annessa al DDL iniziale (*ex* articolo 17) conferma che l'articolo interviene sul decreto-legge 14 giugno 2021, n. 82, prevedendo 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 n. 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).

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 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.

Al riguardo, premesso che le norme si limitano a disciplinare i rapporti tra l'Agenzia, il procuratore nazionale antimafia e antiterrorismo ed il pubblico ministero, si conviene con la RT in merito al tenore ordinamentale della disposizione. Pertanto, nulla da osservare.

Articolo 23
(Verifica della sicurezza negli accessi alle banche dati presso gli uffici giudiziari)

L'articolo, aggiunto in prima lettura, stabilisce che in occasione delle ispezioni da parte del Ministero della giustizia presso gli uffici giudiziari, sia sempre verificato il rispetto delle prescrizioni di sicurezza negli accessi alle banche dati in uso. A tal fine, novella l'articolo 7 della legge 12 agosto 1962, n. 1311:

- la lettera *a)* riguarda le ispezioni ordinarie di cui al primo comma del citato art. 7, che sono disposte dal capo dell'ispettorato generale in tutti gli uffici giudiziari, conformemente alle direttive impartite dal Ministro della giustizia, allo scopo di accertare se i servizi procedono secondo le leggi, i regolamenti e le istruzioni vigenti. Nell'ambito di tali ispezioni, attraverso la modifica introdotta, si prevede che sia effettuata anche la verifica delle prescrizioni di sicurezza negli accessi alle banche dati;

- la lettera *b)* interessa le ispezioni parziali di cui al terzo comma dell'art. 7, che sono disposte dal Ministro della giustizia negli uffici giudiziari quando egli lo ritenga opportuno, allo scopo di verificare la produttività degli stessi nonché l'entità e la tempestività del lavoro di singoli magistrati. In base alla modifica apportata, simili ispezioni possono essere volte altresì all'accertamento del rispetto delle prescrizioni di sicurezza negli accessi alle banche di dati in uso presso i medesimi uffici giudiziari.

L'integrazione è al momento sprovvista di **RT.**

Durante l'esame in prima lettura, il Governo ha affermato che "le verifiche ispettive richieste all'Ispettorato Generale del Ministero della giustizia in ragione delle nuove disposizioni introdotte dal provvedimento in esame, finalizzate al rispetto delle prescrizioni di sicurezza nell'accesso alle banche dati in uso presso gli uffici giudiziari, potranno essere svolte nell'ambito dell'ordinario programma ispettivo annuale a valere sulle risorse disponibili a legislazione vigente" [8].

Al riguardo, va rilevato che le norme prevedono che le verifiche ispettive svolte presso gli uffici giudiziari riguardino d'ora innanzi anche il rispetto delle prescrizioni di sicurezza negli accessi alle banche di dati in uso presso gli uffici stessi.

Per i profili di quantificazione, alla luce delle rassicurazioni pervenute nel corso dell'esame in prima lettura, non ci sono osservazioni.

Articolo 24
(Disposizioni finanziarie)

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

Al comma 2 si stabilisce che i proventi delle sanzioni di cui all'articolo 1, comma 6, confluiscono nelle entrate dell'Agenzia per la cybersicurezza nazionale.

La RT annessa al DDL iniziale ribadisce il contenuto della disposizione.

Al riguardo, quanto al comma 1, richiamando il comma 6-*bis* dell'articolo 17 della legge di contabilità, si rileva che la mera apposizione di clausole di neutralità non costituisce garanzia dell'assenza di nuovi o maggiori oneri, se non alla luce di una RT recante l'illustrazione degli elementi informativi e dei dati finanziari e contabili idonei a comprovarne la sostenibilità, come più volte segnalato dalla Corte dei conti, in un'ottica volta a preservare la piena sostenibilità degli equilibri di finanza pubblica[9].

---

[8] Cfr. Ministero dell'economia e delle finanze, Appunto dell'Ufficio del coordinamento legislativo, in Camera dei deputati, Bollettino delle Giunte e delle Commissioni parlamentari, 14 maggio 2024, pagina 47.

[9] Nell'ultima relazione quadrimestrale della Corte dei conti si legge che" la mancata previsione, infatti, di costi aggiuntivi non esclude che possano effettivamente derivare dalle norme, in futuro, maggiori esigenze a legislazione vigente, con copertura a carico dei "tendenziali" e dunque aggravando il saldo, soprattutto a fronte

Sul piano metodologico, si ricorda che le dotazioni in bilancio dovrebbero scontare esclusivamente i fabbisogni di spesa già previsti ai sensi della normativa vigente[10], dovendo escludersi margini di adeguamento previsti anticipatamente in vista dell'approvazione di nuove norme.

A tale proposito, pur considerando che all'Autorità per la cybersicurezza nazionale è riconosciuta autonomia contabile e di bilancio, va comunque rilevato che la dotazione relativa al suo funzionamento è pressoché integralmente posta a carico del bilancio dello Stato[11].

Sul comma 2, nulla da osservare.

---

di oneri di carattere obbligatorio. Tutto ciò a meno di non ritenere che le disponibilità di bilancio a legislazione vigente siano quantificate in modo da presentare già margini per la copertura di eventuali incrementi di oneri conseguenti all'implementazione delle nuove normative previste: in tal caso si determinerebbe, però, una scarsa coerenza con il principio della legislazione vigente, che, anche nel nuovo sistema contabile, costituisce il criterio per la costruzione delle previsioni di bilancio al netto della manovra, come attesta la presenza, nella legge di bilancio, della Sezione II, dedicata, appunto, alla legislazione vigente". Cfr. Corte dei conti, SS.RR. in sede di controllo, Relazione quadrimestrale sulla tipologia delle coperture e sulle tecniche di quantificazione degli oneri nel quadrimestre, maggio-agosto 2023, Delibera n. 32/2023, pagine 3 e seguenti.

[10] In presenza di clausole di neutralità, anche il Dipartimento della RGS evidenzia che la RT "dovrà riportare i dati e gli elementi che giustifichino l'ipotesi di una assenza di effetti negativi sui saldi di finanza pubblica, fornendo indicazione delle risorse già previste in bilancio utilizzabili per le finalità indicate". Cfr. Ministero dell'economia e delle finanze, Dipartimento della R.G.S., I.G.B., Circolare n. 32/2010, Paragrafo 4.3, pagina 4.

[11] Sul punto, va segnalato che il bilancio di previsione (*budget economico*) dell'ACN per il 2023 (ultimo disponibile) evidenziava che su un valore della produzione di 119 milioni di euro per il medesimo anno, 65,6 milioni erano a carico del bilancio dello Stato, a titolo di contributo ordinario, e i restanti 43,8 milioni di euro a valere su finanziamenti dell'UE (PNRR). I capitoli dello stato di previsione del Ministero dell'economia e delle finanze interessati sono i seguenti: n. 1672 (dotazione funzionamento); n. 3081 (Progetti); n. 7572 (Strategia). Cfr. Agenzia per la cybersicurezza nazionale (ACN), Deliberazione del direttore generale del 31 ottobre 2022, Allegato *budget* economico, pagine 12 e 17, approvato con DPCM 19 dicembre 2022; Ministero dell'economia e delle finanze, Dipartimento della R.G.S., bilancio dello Stato 2024-2026, stato di previsione del Ministero dell'economia e delle finanze, sul sito *internet* del dipartimento.

Ultimi dossier del Servizio del Bilancio

Mar 2024	Nota di lettura n. 137 Schema di decreto legislativo concernente disposizioni integrative e correttive al decreto legislativo 10 ottobre 2022, n. 149, recante attuazione della legge 26 novembre 2021, n. 206, recante delega al Governo per l'efficienza del processo civile e per la revisione della disciplina degli strumenti di risoluzione alternativa delle controversie e misure urgenti di razionalizzazione dei procedimenti in materia di diritti delle persone e delle famiglie nonché in materia di esecuzione forzata (**Atto del Governo n. 137**)
"	Nota di lettura n. 139 Schema di decreto legislativo recante revisione del sistema sanzionatorio tributario (**Atto del Governo n. 144**)
Apr. 2024	Nota di lettura n. 138 **A.S. 1053**: "Misure in materia di ordinamento, organizzazione e funzionamento delle Forze di polizia, delle Forze armate nonché del Corpo nazionale dei vigili del fuoco"
"	Nota di lettura n. 140 **A.S. 1092**: "Conversione in legge del decreto-legge 29 marzo 2024, n. 39, recante misure urgenti in materia di agevolazioni fiscali di cui agli articoli 119 e 119-ter del decreto-legge 19 maggio 2020, n. 34, convertito, con modificazioni, dalla legge 17 luglio 2020, n. 77, altre misure urgenti in materia fiscale e connesse a eventi eccezionali, nonché relative all'amministrazione finanziaria"
"	Documentazione di finanza pubblica n. 12 Documento di economia e finanza 2024 (**Doc. LVII, n. 2**)
"	Nota di lettura n. 141 **A.S. 1110**: "Conversione in legge, con modificazioni, del decreto-legge 2 marzo 2024, n. 19, recante ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR)"
"	Nota di lettura n. 142 Schema di decreto legislativo recante adeguamento della disciplina sanzionatoria prevista dal testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza, di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, al regolamento (UE) n. 1259/2013 che modifica il regolamento (CE) n. 111/2005, recante norme per il controllo del commercio dei precursori di droghe tra la Comunità e i paesi terzi (**Atto del Governo n. 149**)
Mag. 2024	Nota di lettura n. 143 **A.S. 1086**: "Interventi in materia di sicurezza stradale e delega al Governo per la revisione del codice della strada, di cui al decreto legislativo 30 aprile 1992, n. 285" (Approvato dalla Camera dei deputati)
"	Nota di lettura n. 144 Schema di decreto legislativo recante semplificazione dei controlli sulle attività economiche (**Atto del Governo n. 150**)
"	Elementi di documentazione n. 4 Il bilancio dello Stato 2024-2026. Una analisi delle spese per missioni e programmi
"	Nota di lettura n. 145 Schema di decreto legislativo recante disposizioni in materia di riordino del sistema nazionale della riscossione (**Atto del Governo n. 152**)
"	Nota di lettura n. 146 **A.S. 1133**: "Conversione in legge del decreto-legge 7 maggio 2024, n. 60, recante ulteriori disposizioni urgenti in materia di politiche di coesione"
"	Nota di lettura n. 147 **A.S. 1054**: "Disposizioni per il riconoscimento e la promozione delle zone montane"

Il testo del presente dossier è disponibile in formato elettronico alla URL http://www.senato.it/documentazione/bilancio