Camera dei deputati

XIX LEGISLATURA

Verifica delle quantificazioni

A.C. 1717-A

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

N. 205 – 14 maggio 2024

Camera dei deputati

XIX LEGISLATURA

Verifica delle quantificazioni

A.C. 1717-A

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

N. 205 – 14 maggio 2024

La verifica delle relazioni tecniche che corredano i provvedimenti all'esame della Camera e degli effetti finanziari dei provvedimenti privi di relazione tecnica è curata dal Servizio Bilancio dello Stato.
La verifica delle disposizioni di copertura è curata dalla Segreteria della V Commissione (Bilancio, tesoro e programmazione).
L'analisi è svolta a fini istruttori, a supporto delle valutazioni proprie degli organi parlamentari, ed ha lo scopo di segnalare ai deputati, ove ne ricorrano i presupposti, la necessità di acquisire chiarimenti ovvero ulteriori dati e informazioni in merito a specifici aspetti dei testi.

SERVIZIO BILANCIO DELLO STATO – Servizio Responsabile
☎ 066760-2174 / 066760-9455 – ✉ *bs_segreteria@camera.it*

SERVIZIO COMMISSIONI – Segreteria della V Commissione
☎ 066760-3545 / 066760-3685 – ✉ *com_bilancio@camera.it*

INDICE

Informazioni sul provvedimento

A.C.	**1717-A**
Titolo:	**Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici**
Iniziativa:	**governativa**
Iter al Senato:	no
Relazione tecnica (RT)	presente
Relatori per le Commissioni di merito:	Pagano (FI-PPE) e Maschio (FDI)
Commissioni competenti:	I Commissione (Affari Costituzionali) e II Commissione (Giustizia)

PREMESSA

Il disegno di legge, di iniziativa governativa, ha ad oggetto disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.
È oggetto della presente Nota il testo, composto di 23 articoli, quale risultante dalle modifiche introdotte nel corso dell'esame, in sede referente, dalle Commissione riunite I (Affari costituzionali) e II (Giustizia).
Il testo originario del provvedimento è corredato di relazione tecnica che risulta ancora utilizzabile.
Si esaminano di seguito le norme considerate dalla relazione tecnica e le altre disposizioni che presentano profili di carattere finanziario.

VERIFICA DELLE QUANTIFICAZIONI

ARTICOLI da 1 a 14
Disposizioni in materia di rafforzamento della cybersicurezza nazionale

Le norme, modificate dalle Commissioni di merito, costituiscono il Capo I che reca disposizioni in materia di rafforzamento della cybersicurezza nazionale, resilienza delle pubbliche amministrazioni, personale e funzionamento dell'Agenzia per la cybersicurezza

nazionale, nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici.

In particolare, sono introdotti i seguenti interventi normativi:

- si stabilisce che le pubbliche amministrazioni centrali, le regioni e le province autonome, di Trento e Bolzano, le città metropolitane, i comuni con popolazione superiore a 100 mila abitanti, le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100 mila abitanti, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane, e le aziende sanitarie locali, comprese le rispettive società *in house*, che forniscono i servizi - espressamente individuati, nel corso dell'esame in sede referente - segnalano e notificano gli incidenti[1] aventi impatto su reti, sistemi informativi e servizi informatici. Le segnalazioni e le notifiche sono effettuate tramite le apposite procedure disponibili nel sito internet istituzionale dell'Agenzia per la cybersicurezza nazionale ("Agenzia" nel seguito della nota). Nel caso di inosservanza dell'obbligo di notifica, l'Agenzia dispone di poteri di ammonimento, impulso, ispettivi e sanzionatori anche di tipo pecuniario. Si prevede, inoltre, con disposizione introdotta dalle Commissioni di merito, che per i comuni con popolazione superiore a 100.000 abitanti e i comuni capoluoghi di regione, per le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, per le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane, per le aziende sanitarie locali e per le società *in house* dianzi menzionate i predetti obblighi si applichino a decorrere dal centottantesimo giorno successivo alla data di entrata in vigore della presente legge. Sono quindi indicati alcuni soggetti a cui non si applicano le norme appena descritte tra cui gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato (articolo 1);
- si prevede che le amministrazioni e gli enti pubblici e altri soggetti destinatari delle norme in esame, qualora siano oggetto di segnalazioni dell'Agenzia circa specifiche vulnerabilità cui essi risultano potenzialmente esposti, debbano provvedere tempestivamente all'adozione degli interventi risolutivi indicati dalla stessa Agenzia. Anche in tal caso l'Agenzia, in caso di inadempienze o ritardi, può irrogare sanzioni (articolo 2);
- si stabilisce che anche i soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica siano soggetti all'obbligo di segnalazione (oltre a quello di notifica, già previsto a legislazione vigente) degli incidenti che intervengono su reti, sistemi informativi e servizi informatici che si trovano al di fuori del Perimetro (articolo 3);

[1] Indicati nella tassonomia di cui all'articolo 1, comma 3-bis, del decreto legge 21 settembre 2019, n. 105.

- si dispone, con una norma introdotta dalle Commissioni di merito, che l'Agenzia debba provvedere all'elaborazione e alla classificazione dei dati relativi alle notifiche di incidenti ricevute. Tali dati sono quindi resi pubblici nell'ambito della relazione prevista dall'articolo 14, comma 1, del decreto-legge n. 82 del 2021[2]. A tali adempimenti si provvede con le risorse umane, strumentali e finanziarie già previste a legislazione vigente (articolo 4);
- si prevede[3] che alle riunioni del Nucleo per la cybersicurezza possano partecipare anche rappresentanti della Direzione nazionale antimafia e antiterrorismo, della Banca d'Italia e altri soggetti, interessati a specifiche questioni di particolare rilevanza (articolo 5);
- si prevede che il Presidente del Consiglio dei ministri possa disporre il differimento degli obblighi informativi e delle attività di resilienza in capo all'Agenzia per la cybersicurezza nazionale nei casi in cui ciò sia considerato strettamente necessario dai servizi di sicurezza della Repubblica (articolo 6);
- si dispone l'integrazione, con una norma inserita dalle Commissioni di merito, della composizione del Comitato interministeriale per la pubblica sicurezza a cui possono partecipare anche il Ministro dell'agricoltura, della sovranità alimentare e delle foreste, il Ministro delle infrastrutture e dei trasporti e il Ministro dell'università e della ricerca (articolo 7);
- si prevede che i soggetti indicati all'articolo 1, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, individuino, ove non sia già presente, una struttura, anche tra quelle esistenti, preposta alle attività di cybersicurezza. Presso le strutture di cui al comma 1 opera il referente per la cybersicurezza. A seguito di modifiche introdotte dalle Commissioni di merito, il referente deve essere in possesso di specifiche e comprovate professionalità e competenze in materia di cybersicurezza e qualora nell'amministrazione non figuri un tale soggetto è possibile conferire l'incarico di referente a un dipendente di una pubblica amministrazione, nell'ambito delle risorse disponibili a legislazione vigente[4] (articolo 8, commi 1 e 2);
- si prevede, con una norma inserita dalle Commissioni di merito, al fine di garantire adeguata tutela e protezione dai rischi di accesso abusivo ai dati contenuti in sistemi informatici delle pubbliche amministrazioni, che per l'accesso alle banche di dati

[2] Si tratta di una relazione che il Presidente del Consiglio dei ministri trasmette al Parlamento entro il 30 aprile di ogni anno sull'attività svolta dall'Agenzia nell'anno precedente, in materia di cybersicurezza nazionale.
[3] Apportando modifiche all'articolo 8 del decreto-legge 14 giugno 2021, n. 82.
[4] Anche in tale caso sono indicati alcuni soggetti cui non si applicano le norme recate dall'articolo 6 appena descritte (articolo 6, comma 6)

pubbliche da parte di addetti tecnici[5] e di soggetti incaricati del trattamento dei dati in esse contenuti è richiesto l'utilizzo di specifici sistemi di autenticazione informatica, consistenti nell'uso combinato di almeno due differenti tecnologie di autenticazione, una delle quali sia basata sull'elaborazione di caratteristiche biometriche. Inoltre, limitatamente ai casi di interventi indifferibili relativi a malfunzionamenti, o aggiornamenti di *hardware* e *software*, che determinino la necessità di accesso ai sistemi informatici, detto accesso è consentito anche senza l'utilizzo di due differenti tecnologie di autenticazione o di una tecnologia di autenticazione biometrica, per le operazioni che richiedono la presenza fisica dell'addetto che procede all'intervento in prossimità del sistema di elaborazione: in questo caso, però, gli accessi sono annotati in un apposito registro unitamente alle motivazioni che li hanno determinati e alla descrizione sintetica delle operazioni svolte. Le modifiche prevedono che le pubbliche amministrazioni adottino misure di sicurezza ora descritte utilizzando le risorse umane, finanziarie e strumentali disponibili a legislazione vigente (articolo 8, commi da 7 a 11);

- si prevede, con una disposizione introdotta dalle Commissioni di merito, che le strutture di cui all'articolo 8 nonché quelle che svolgono analoghe funzioni per i soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge n. 105 del 2019, e al decreto legislativo 18 maggio 2018, n. 65[6], verificano che i programmi e le applicazioni informatiche e di comunicazione elettronica in uso, che utilizzano soluzioni crittografiche, rispettino le linee guida sulla crittografia nonché quelle sulla conservazione delle *password* adottate dall'Agenzia per la cybersicurezza nazionale e dal Garante per la protezione dei dati personali e che non comportino vulnerabilità note, atte a rendere disponibili e intellegibili a terzi i dati cifrati (articolo 9);
- si dispone, per effetto delle modifiche introdotte all'articolo 10 dalle Commissioni di merito, il potenziamento delle funzioni dell'Agenzia in materia di crittografia[7] e l'istituzione presso l'Agenzia stessa del Centro nazionale di crittografia, disciplinato con provvedimento del direttore generale di quest'ultima;
- si prevede l'adozione da parte dell'Agenzia di un regolamento che stabilisca termini e modalità per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia (articolo 11);

---

[5] Per «addetti tecnici» si intendono gli operatori tecnici aventi funzioni di amministratori di sistema, di rete o di archivio di dati.

[6] Ossia per i soggetti rientranti nell'ambito del perimetro di sicurezza nazionale cibernetica e per gli operatori di servizi essenziali con sede nel territorio nazionale identificati per ciascun settore e sotto settore, indicati nell'allegato II del citato decreto legislativo n. 65 del 2018, dalle autorità competenti NIS (*Network and information security*) con propri provvedimenti.

[7] Sostituendo la lettera *m*-bis) dell'articolo 7, comma 1, del decreto-legge 14 giugno 2021, n. 82.

- si stabilisce che 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, per la durata di due anni a decorrere dalla data di completamento dell'ultimo dei predetti percorsi formativi non possono essere assunti né assumere incarichi presso soggetti privati al fine di svolgere mansioni in materia di cybersicurezza[8] (articolo 12, comma 1, capoverso 8-*ter*);
- si prevede, con una norma introdotta dalle Commissioni di merito, che il personale dell'Agenzia proveniente dalle Forze armate o dalle Forze di polizia possa rientrare, per motivate esigenze operative, nel ruolo dell'amministrazione di originaria provenienza, su richiesta della stessa, con l'assenso dell'interessato e del direttore generale dell'Agenzia. In caso di rientro, agli effetti relativi alla progressione di carriera, all'avanzamento e allo stato giuridico del personale proveniente dalle citate amministrazioni si provvede con regolamento da adottare con DPCM, previo parere delle Commissioni parlamentari competenti per materia e per i profili finanziari. Tali disposizioni si applicano nel rispetto del quadro ordinamentale di riferimento, nei limiti delle facoltà assunzionali delle amministrazioni interessate, senza nuovi o maggiori oneri per il bilancio dello Stato e senza determinare posizioni sovrannumerarie e riconoscimento di differenziali economici (articolo 12, comma 1, capoverso 8-*quater*);
- si prevede che, con decreto del presidente del Consiglio dei ministri da adottare entro 120 giorni dalla data di entrata in vigore del presente provvedimento, siano individuati gli elementi essenziali di cybersicurezza per specifiche categorie di beni e servizi informatici[9] che le amministrazioni pubbliche, le società pubbliche e i soggetti privati compresi nel perimetro di sicurezza cibernetica devono tenere in considerazione nelle attività di approvvigionamento di beni e servizi informatici da essi impiegati[10] (articolo 13);
- viene integrato, con una norma introdotta dalle Commissioni di merito, il testo dell'articolo 16 della legge n. 15 del 2024 (legge di delegazione europea 2022-2023)[11].

---

[8] Tali disposizioni non si applicano al personale cessato dal servizio presso l'Agenzia secondo quanto previsto dalle disposizioni del regolamento adottato ai sensi del presente articolo relative al collocamento a riposo d'ufficio, al raggiungimento del requisito anagrafico previsto dalla legge per la pensione di vecchiaia, alla cessazione a domanda per inabilità o alla dispensa dal servizio per motivi di salute.

[9] Si segnala che il riferimento alle specifiche categorie di beni e servizi informatici è stato inserito dalle Commissioni di merito.

[10] Le norme precisano che per elementi essenziali di cybersicurezza si intende l'insieme di criteri e regole tecniche il cui rispetto garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela degli interessi strategici nazionali.

[11] Si rammenta che il citato articolo 16 ha delegato il Governo ad adottare uno o più decreti legislativi per l'adeguamento della normativa nazionale al regolamento (UE) 2022/2554 e per il recepimento della direttiva (UE) 2022/2556 relativi alla resilienza operativa digitale per il settore finanziario. Ai sensi del comma 3 del medesimo articolo, dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni

Le integrazioni aggiungono un nuovo criterio direttivo volto a conseguire un livello elevato di resilienza operativa digitale e assicurare la stabilità del settore finanziario definendo adeguati presìdi in materia di resilienza operativa digitale e attribuendo alla Banca d'Italia l'esercizio nei confronti dei soggetti di cui alla presente lettera dei poteri di vigilanza, di indagine e sanzionatori (articolo 14).

La relazione tecnica, riferita al testo originario del provvedimento, ribadisce il contenuto delle norme e afferma che gli articoli del Capo I non comportano nuovi o maggiori oneri a carico della finanza pubblica e che le amministrazioni pubbliche interessate provvedono agli adempimenti previsti dagli articoli 1, 2, 5, 6, 8, 10, e 11[12] con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Con specifico riferimento alle sanzioni previste dall'articolo 1, comma 5, la relazione tecnica non ritiene possibile esprimere una previsione in merito all'eventuale gettito, evidenziando, però, che le eventuali nuove entrate sono di pertinenza dell'Agenzia ai sensi dell'articolo 11, comma 2, lettera *f)*, del decreto-legge n. 82 del 2021.

Si rammenta che, ai sensi della lettera *f)* ora citata, costituiscono entrate dell'Agenzia, oltre alle altre fonti elencate nel comma 2 prima menzionato, i proventi delle sanzioni irrogate dall'Agenzia ai sensi di quanto previsto dal decreto legislativo n. 65 del 2018, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione europea (cd. "decreto legislativo NIS"), dal decreto-legge n. 105 del 2019, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica (cd. "decreto-legge perimetro") e dal decreto legislativo 1° agosto 2003, n. 259, recante il Codice delle comunicazioni elettroniche, e relative disposizioni attuative.

Con riferimento all'articolo 8, comma 2[13], che prevede l'istituzione del referente per la cybersicurezza nell'ambito del personale delle amministrazioni pubbliche interessate dall'applicazione delle disposizioni in esame, la relazione tecnica precisa che l'incarico in questione non dà diritto a compensi aggiuntivi.

In merito ai profili di quantificazione, si rileva preliminarmente che le disposizioni in esame sono volte a potenziare la sicurezza delle reti, dei sistemi informativi e dei servizi informatici. A tal fine è disposto che una pluralità di soggetti, in gran parte amministrazioni pubbliche, sia tenuto a segnalare e notificare all'Agenzia per la cybersicurezza nazionale gli

competenti provvedono all'adempimento dei compiti derivanti dall'esercizio della delega di cui al presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

[12] Si fa riferimento alla numerazione degli articoli del testo A che diverge da quella del disegno di legge originario.

[13] Nel testo originario si trattava dell'articolo 6, comma 2.

incidenti che concernono le citate reti e sistemi informativi e sono disciplinati ulteriori poteri di ammonimento, impulso, ispettivi e sanzionatori attribuiti all'Agenzia. Le norme prevedono, altresì, che determinate amministrazioni pubbliche individuino, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e ove non sia già presente, una struttura, anche tra quelle esistenti, preposta alle attività di cybersicurezza presso cui opera il referente per la cybersicurezza. Il testo originario del provvedimento stabiliva che il citato referente dovesse essere individuato "in ragione delle qualità professionali possedute" e la relazione tecnica precisava che ad esso non competono compensi aggiuntivi, mentre il testo risultante dalle modifiche introdotte dalle Commissioni di merito prevede il possesso di "specifiche e comprovate professionalità e competenze in materia di cybersicurezza" e, ove non si disponga di tale personale, si prevede 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.

Ulteriori disposizioni introdotte dalle Commissioni di merito prevedono:

- il rafforzamento da parte delle pubbliche amministrazioni, mediante specifici sistemi di autenticazione informatica, della tutela e della protezione dei propri sistemi informativi e delle proprie banche dati dai rischi di accesso abusivo;
- il potenziamento delle funzioni dell'Agenzia in materia di crittografia con l'istituzione, presso la stessa, del Centro nazionale di crittografia, disciplinato con provvedimento del suo direttore generale;
- la possibilità per il personale dell'Agenzia proveniente dalle Forze armate o dalle Forze di polizia di rientrare nel ruolo dell'amministrazione di originaria provenienza, su richiesta della stessa, con l'assenso dell'interessato e del direttore generale dell'Agenzia; in caso di rientro gli effetti relativi alla progressione di carriera, all'avanzamento e allo stato giuridico del personale proveniente dalle citate amministrazioni, si provvede con regolamento da adottare con DPCM, previo parere, fra l'altro, delle Commissioni parlamentari competenti per i profili finanziari; tali disposizioni si applicano, secondo quanto specificato dalle stesse, nei limiti delle facoltà

assunzionali delle amministrazioni interessate, senza nuovi o maggiori oneri per il bilancio dello Stato e senza determinare posizioni sovrannumerarie e riconoscimento di differenziali economici;

- l'integrazione del testo dell'articolo 16 della legge n. 15 del 2024 (legge di delegazione europea 2022-2023) che reca la delega al Governo ad adottare uno o più decreti legislativi per l'adeguamento della normativa nazionale al regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, nonché per il recepimento della direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativi alla resilienza operativa digitale per il settore finanziario.

Tanto premesso, si prende atto che la relazione tecnica con riferimento alle norme originarie del provvedimento afferma che le stesse non comportano nuovi o maggiori oneri a carico della finanza pubblica e che le amministrazioni pubbliche interessate provvedono alla loro attuazione con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente e che dunque anche il potenziamento dei compiti assegnati all'Agenzia e l'eventuale istituzione di una struttura preposta alle attività di cybersicurezza in determinate pubbliche amministrazioni possano realizzarsi mediante l'impiego delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente. Appare, tuttavia, necessario che il Governo confermi che possano essere svolti, a valere sulle risorse disponibili, anche gli ulteriori adempimenti amministrativi derivanti dalle seguenti disposizioni introdotte durante l'esame in sede referente:

- l'articolo 4 che prevede che l'Agenzia debba provvedere all'elaborazione e alla classificazione dei dati relativi alle notifiche di incidenti ricevute;
- l'articolo 6, commi da 7 a 11, che prevedono che le pubbliche amministrazioni debbano rafforzare, mediante specifici sistemi di autenticazione informatica, la tutela e la protezione dei propri sistemi informativi e delle proprie banche dati dai rischi di accesso abusivo utilizzando le risorse umane, finanziarie e strumentali disponibili a legislazione vigente;

- l'articolo 10, come modificato dalle Commissioni di merito, che prevede il potenziamento delle funzioni dell'Agenzia in materia di crittografia e l'istituzione, presso l'Agenzia, del Centro nazionale di crittografia.

Inoltre, con rifermento alla figura del referente per la cybersicurezza dovrebbe essere valutata la necessità di precisare nel testo del provvedimento quanto affermato dalla relazione tecnica con riferimento alla norma contenuta nel testo originario - ossia che al referente non spettano compensi aggiuntivi - mediante l'inserimento della consueta clausola di invarianza finanziaria relativa all'esclusione degli emolumenti. Su tale aspetto appare comunque necessario acquisire l'avviso del Governo.

Non si hanno invece osservazioni da formulare per quanto concerne la possibilità per il personale dell'Agenzia proveniente dalle Forze armate o dalle Forze di polizia di rientrare nel ruolo dell'amministrazione di originaria provenienza, considerato che il rientro può essere disposto nei limiti delle facoltà assunzionali delle amministrazioni interessate, senza nuovi o maggiori oneri per il bilancio dello Stato e senza determinare posizioni sovrannumerarie e riconoscimento di differenziali economici.

Analogamente, non si hanno osservazioni da formulare anche con riguardo alle norme che integrano il testo dell'articolo 16 della legge n. 15 del 2024 (legge di delegazione europea 2022-2023) in materia di resilienza operativa digitale per il settore finanziario, tenuto conto della natura prevalentemente ordinamentale delle disposizioni, per altro assistite da una specifica clausola di invarianza finanziaria.

In merito ai profili di copertura finanziaria, si rileva che il comma 11 dell'articolo 8 prevede una clausola di invarianza finanziaria in base alla quale all'attuazione delle disposizioni del presente articolo si provvede con le risorse umane, finanziarie e strumentali disponibili a legislazione vigente. In proposito, nel rilevare che la predetta clausola appare formulata correttamente, si segnala che il provvedimento è corredato, all'articolo 23, comma 1, di una clausola di invarianza finanziaria riferita all'intero disegno di legge. Si potrebbe, quindi, valutare

l'opportunità di coordinare le due disposizioni. Sul punto appare comunque opportuno acquisire l'avviso del Governo.

ARTICOLI da 15 a 17

Potenziamento del contrasto dei reati informatici – norme penali, di procedura penale e sui collaboratori di giustizia

Le norme ampliano l'ambito di applicazione di alcune fattispecie disciplinate dal codice penale e inaspriscono, con riferimento ai reati informatici o perpetrati con mezzi informatici, il trattamento sanzionatorio per queste previsto.

Sono quindi modificati o introdotti numerosi articoli del codice penale tra cui i seguenti:

- l'articolo 615-*ter*, accesso abusivo a un sistema informatico o telematico [articolo 15, comma 1, lettera *b*)];
- l'articolo 615-*quater*, detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici [articolo 15, comma 1, lettera *c*)];
- l'articolo 617-*bis*, detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche e telefoniche [articolo 15, comma 1, lettera *e*)];
- l'articolo 617-*quater*, intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche [articolo 15, comma 1, lettera *f*)];
- l'articolo 617-*quinquies*, detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche [articolo 15, comma 1, lettera *g*)];
- l'articolo 617-*sexies*, falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche [articolo 15, comma 1, lettera *h*)];
- l'articolo 629, estorsione [articolo 15, comma 1, lettera *m*)];
- l'articolo 635-*bis*, danneggiamento di informazioni, dati e programmi informatici [articolo 15, comma 1, lettera *n*)];
- l'articolo 635-*ter*, danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità [articolo 15, comma 1, lettera *o*)];
- l'articolo 635-*quater* danneggiamento di sistemi informatici o telematici [articolo 15, comma 1, lettera *p*)];
- l'articolo 635-*quater*.1, detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico [articolo 15, comma 1, lettera *q*)];
- l'articolo 635-*quinquies*, danneggiamento di sistemi informatici o telematici di pubblico interesse [articolo 15, comma 1, lettera *r*)];

- l'articolo 640, truffa [articolo 15, comma 1, lettera *t*)].

Sono inoltre apportate modifiche al codice di procedura penale finalizzate a recepire gli interventi in materia di prevenzione e contrasto dei reati informatici introdotte dal precedente articolo 15. 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 (articolo 16).

Infine, attraverso alcune modifiche al decreto-legge n. 8 del 1991 si estende il campo di applicazione delle disposizioni di protezione dei soggetti che collaborano con la giustizia anche agli autori dei reati informatici più gravi (articolo 17).

La relazione tecnica evidenzia che le disposizioni in esame hanno carattere ordinamentale e precettivo e non sono suscettibili di determinare nuovi o maggiori oneri a carico della finanza pubblica. In particolare, per quanto concerne le modifiche al codice di procedura penale la relazione tecnica sottolinea che 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.

In merito ai profili di quantificazione, si rileva preliminarmente che le norme in esame sono finalizzate al potenziamento del contrasto dei reati informatici: a tal fine si amplia l'ambito di applicazione di alcune fattispecie disciplinate dal codice penale e si inasprisce il trattamento sanzionatorio previsto per queste ultime con riferimento ai reati informatici o perpetrati con mezzi informatici. Sono inoltre apportate modifiche al codice di procedura penale per rendere più efficace la repressione di detti reati e si stabilisce, attraverso modifiche al decreto-legge n. 8 del 1991, che si estende il campo di applicazione delle disposizioni di protezione dei soggetti che collaborano con la giustizia anche agli autori dei reati informatici più gravi. Ciò posto, appare necessario che il Governo fornisca elementi di valutazione di carattere amministrativo-contabile, volti ad assicurare 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.

ARTICOLO 18

Potenziamento del contrasto dei reati informatici – norme sulle intercettazioni

Le norme, attraverso una modifica al decreto-legge n. 152 del 1991, estendono la disciplina delle intercettazioni prevista per i fatti di criminalità organizzata ai reati informatici rimessi al coordinamento del procuratore nazionale antimafia e antiterrorismo.

La relazione tecnica ribadisce il contenuto delle norme ed esplicita che la finalità è quella di consentire una più efficace e tempestiva azione diretta all'accertamento delle attività delittuose, prevedendo la possibilità di disporre le operazioni di intercettazione in presenza di sufficienti indizi. Dal punto di vista finanziario la norma, secondo la relazione tecnica, 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 nello stato di previsione della spesa 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.
La relazione tecnica 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.

In merito ai profili di quantificazione, si rileva preliminarmente che le norme in esame estendono la disciplina delle intercettazioni prevista per i fatti di criminalità organizzata ai reati informatici rimessi al coordinamento del procuratore nazionale antimafia e antiterrorismo.
A questo riguardo la relazione tecnica afferma che la norma 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 iscritte sul programma di spesa 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" (capitolo 1363), per un ammontare pari a 212.143.598 euro per ciascuno degli anni del triennio 2024-2026, anche perché recenti interventi normativi, volti alla

razionalizzazione e al contenimento delle tariffe sia delle prestazioni obbligatorie che di quelle funzionali alle operazioni di intercettazione, determineranno risparmi di spesa.

A questo riguardo si evidenzia tuttavia che, 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[14].

A questo riguardo, trattandosi di spese obbligatorie le somme eventualmente necessarie per aumentarne il relativo stanziamento sono trasferite, con decreti del Ministro dell'economia e delle finanze, da registrare alla Corte dei conti, dal fondo di riserva per le spese obbligatorie ed iscritte in aumento delle dotazioni sia di competenza sia di cassa delle competenti unità elementari di bilancio, ai fini della gestione e della rendicontazione (articolo 26 della legge n. 196 del 2009, in materia di contabilità e finanza pubblica).

In questo quadro, si rammenta infine che il citato 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.

La predetta ricostruzione, basata sul rendiconto dell'ultimo esercizio disponibile, sembrerebbe quindi evidenziare l'insufficienza dello stanziamento iniziale riferito all'anno 2022 per far fonte agli impegni derivanti dalla legislazione allora vigente, tanto che se ne era dovuto integrare l'ammontare nel corso dell'esercizio e che l'importo così integrato – per altro superiore allo stanziamento riferito all'anno 2024 - era stato comunque quasi completamente impegnato.

Tutto ciò considerato, pur prendendosi atto delle misure di razionalizzazione della spesa indicate dalla relazione tecnica, comunque già da tempo vigenti, dovrebbero essere forniti dal Governo ulteriori elementi di carattere amministrativo-contabile volti a garantire che, nel corso del presente esercizio e possibilmente a regime, vi siano margini di risorse inutilizzate che risultino quantitativamente idonee, da un lato, ad escludere il ricorso durante l'esercizio a prelievi dal fondo di riserva per spese obbligatorie e, dall'altro, a far fronte anche alle nuove esigenze finanziarie derivanti dal maggior numero di intercettazioni.

[14] Salvo economie di spesa di soli 2.406,25 euro.

ARTICOLO 19

Potenziamento del contrasto dei reati informatici – responsabilità amministrativa degli enti

Le norme modificano il decreto legislativo n. 231 del 2001, che disciplina la responsabilità amministrativa delle persone giuridiche. Le modifiche riguardano l'articolo 24-*bis*, che tratta dei delitti informatici e del trattamento illecito di dati, e inaspriscono le sanzioni a cui sono assoggettati gli enti qualora reputati responsabili di tali eventi.

La relazione tecnica 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, e così via, generando possibili effetti positivi per la finanza pubblica dovuti all'incremento delle sanzioni pecuniarie, sebbene allo stato non quantificabili.

In merito ai profili di quantificazione, si rileva preliminarmente 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. Ciò posto, considerato il carattere ordinamentale delle disposizioni e il fatto che non vengono scontati effetti finanziari positivi derivanti dall'incremento delle sanzioni, non si formulano osservazioni.

ARTICOLO 20

Procedura per la protezione dei testimoni di giustizia in caso di reati informatici

Le norme intervengono[15] sul procedimento di applicazione delle speciali misure di protezione per i testimoni di giustizia e per gli altri protetti, prevedendo che la Commissione centrale per la definizione e applicazione delle speciali misure di protezione debba richiedere il parere al Procuratore nazionale antimafia e antiterrorismo sulla proposta di ammissione alle speciali misure, anche nel caso dei gravi delitti informatici.

La relazione tecnica afferma che la norma ha natura ordinamentale e procedurale e non è suscettibile determinare nuovi o maggiori oneri per la finanza pubblica, atteso che tali

[15] Attraverso una modifica dell'articolo 11 della legge n. 6 del 2018 sulla protezione dei testimoni di giustizia.

adempimenti rientrano fra le ordinarie attività istituzionali e pertanto, potranno essere garantiti con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

In merito ai profili di quantificazione, si rileva preliminarmente che le norme in esame prevedono che la Commissione centrale per la definizione e applicazione delle speciali misure di protezione debba richiedere il parere al Procuratore nazionale antimafia e antiterrorismo sulla proposta di ammissione alle speciali misure di protezione dei testimoni, anche nel caso dei gravi delitti informatici. Ciò posto, considerato il carattere ordinamentale delle disposizioni, non si hanno pertanto osservazioni da formulare.

ARTICOLO 21
Rapporti dell'Agenzia per la cybersicurezza nazionale e operatori della giustizia

Le norme integrano il testo dell'articolo 17 del decreto-legge n. 82 del 2021[16], disciplinando i rapporti tra l'Agenzia per la cybersicurezza nazionale il procuratore nazionale antimafia e antiterrorismo ed il pubblico ministero.
In particolare, si prevede che nei casi in cui l'Agenzia abbia notizia di un attacco ai sistemi informatici o telematici di particolari soggetti, la stessa ne informa senza ritardo il procuratore nazionale antimafia e antiterrorismo e procede alle attività di analisi e risposta agli attacchi che gli competono
Analogamente quando il pubblico ministero acquisisce la notizia di alcuni gravi delitti informatici deve darne tempestiva informazione all'Agenzia assicurando anche il raccordo informativo con l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione. Più in generale si dispone che il pubblico ministero nello svolgimento delle sue attività di indagine sui delitti in questione deve tenere conto delle attività che sulle medesime questioni sono svolte dall'Agenzia.

La relazione tecnica afferma che le disposizioni in questione 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 tra diversi soggetti pubblici, 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.

[16] Che reca disposizioni urgenti in materia di cyber-sicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.

In merito ai profili di quantificazione si rileva preliminarmente che le norme in esame disciplinano i rapporti tra l'Agenzia, il procuratore nazionale antimafia e antiterrorismo ed il pubblico ministero. Ciò stante, considerato il carattere ordinamentale delle disposizioni, non si hanno osservazioni da formulare.

ARTICOLO 22
Funzionamento dell'Ispettorato generale presso il Ministero di grazia e giustizia.

Le norme, introdotte dalle Commissioni di merito, modificano la legge 12 agosto 1962, n. 1311, in materia di organizzazione e funzionamento dell'Ispettorato generale presso il Ministero di grazia e giustizia. Le modifiche riguardano l'articolo 7 concernente le verifiche ispettive e stabiliscono che nel corso di queste ultime è oggetto di valutazione anche il rispetto delle prescrizioni di sicurezza negli accessi alle banche di dati in uso presso gli uffici giudiziari.

La relazione tecnica non considera la norma che è stata introdotta nel corso dell'esame parlamentare.

In merito ai profili di quantificazione, si rileva preliminarmente che le norme in esame stabiliscono che le verifiche ispettive svolte presso gli uffici giudiziari riguardano anche il rispetto delle prescrizioni di sicurezza negli accessi alle banche di dati in uso presso gli uffici stessi. Al riguardo appare necessario che il Governo assicuri che le più ampie attività ispettive prescritte dalle disposizioni di cui trattasi possano essere svolte nell'ambito delle risorse disponibili a legislazione vigente.

ARTICOLO 23
Disposizioni finanziarie

Le norme stabiliscono che dall'attuazione della presente legge non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e che le amministrazioni pubbliche competenti provvedono all'adempimento dei compiti derivanti dalla presente legge con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente (comma 1).
Si stabilisce che i proventi delle sanzioni di cui all'articolo 1, comma 5, confluiscono nelle entrate dell'Agenzia per la cybersicurezza nazionale.

La relazione tecnica ribadisce il contenuto delle norme.

In merito ai profili di quantificazione, si rileva preliminarmente che le norme in esame recano la clausola di invarianza finanziaria riferita all'intero provvedimento e prevedono che i proventi delle sanzioni di cui all'articolo 1, comma 5, confluiscono nelle entrate dell'Agenzia per la cybersicurezza nazionale. Ciò stante, non si hanno osservazioni da formulare.

In merito ai profili di copertura finanziaria, si rileva che il comma 1 prevede una clausola di invarianza finanziaria riferita all'intero disegno di legge, in base alla quale dall'attuazione del provvedimento non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e le amministrazioni interessate vi provvedono nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente. In proposito, non si hanno osservazioni sulla formulazione della disposizione.

Il comma 2 prevede infine che i proventi delle sanzioni di cui all'articolo 1, comma 5, confluiscono nelle entrate dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 11, comma 2, lettera *f)*, del decreto-legge n. 82 del 2021. In proposito, si ricorda che, sotto il profilo contabile, i proventi di cui all'articolo 11, comma 2, del citato decreto-legge n. 82 del 2021, sono versati, ai sensi dell'articolo 18, comma 4, del medesimo decreto, all'entrata del bilancio dello Stato, per essere riassegnati al capitolo di bilancio relativo al finanziamento dell'Agenzia per la cybersicurezza nazionale, di cui al comma 1 del medesimo articolo 18. Al riguardo, non si hanno pertanto osservazioni in ordine alla formulazione della disposizione.