**BOZZE DI STAMPA**
**3 agosto 2021**
**N. 1**

# SENATO DELLA REPUBBLICA

## XVIII LEGISLATURA

**Conversione in legge, con modificazioni, del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale (2336)**

## ORDINI DEL GIORNO

### Art. 4

**G4.100**
RAUTI, MALAN

Il Senato,

premesso che:

L'articolo 4 del presente provvedimento istituisce, presso la Presidenza del Consiglio dei ministri, il Comitato interministeriale per la cybersicurezza (CIC), organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza;

impegna il governo:

a valutare, compatibilmente con gli equilibri di finanza pubblica, l'opportunità di adottare iniziative volte all'individuazione, nell'ambito dell'Agenzia, di una struttura di coordinamento per la cybersicurezza che possa fungere da raccordo per le istanze delle singole amministrazioni in questo settore.

**G4.101**
RAUTI, MALAN

Il Senato,

premesso che:

il provvedimento assegna al Comitato interministeriale per la cybersicurezza all'articolo 4, comma 2, lettera c) la promozione dell'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza;

considerato che il processo di procurement degli operatori privati interessati alla cybersicurezza ricadenti all'interno del perimetro di sicurezza nazionale cibernetica sconta delle criticità in termini di trasparenza e accountability soprattutto con riguardo ai servizi offerti dalle PMI,

impegna il Governo

a valutare l'opportunità, compatibilmente con gli equilibri di finanza pubblica, di istituire un Registro nazionale degli operatori di cybersicurezza, con particolare riferimento alle realtà emergenti e quelle con capacità di ricerca e sviluppo sul territorio nazionale, per contribuire a definire i requisiti delle professionalità e delle competenze da sviluppare e a mappare le capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta con l'obiettivo di supportarne la crescita.

---

**G4.102**
MALLEGNI

Il Senato,

in sede di discussione deldecreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale;

premesso che:

l'articolo 4 del decreto istituisce, presso la Presidenza del Consiglio dei ministri, il "Comitato interministeriale per la cybersicurezza" (CIC), organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza;

il comma 3 del citato articolo reca la composizione del Comitato come segue: il Presidente del Consiglio che lo presiede; l'Autorità delegata, ove istituita; il Ministro degli affari esteri e della cooperazione internazionale;

il Ministro dell'interno; il Ministro della giustizia; il Ministro della difesa; il Ministro dell'economia e delle finanze; il Ministro dello sviluppo economico; il Ministro della transizione ecologica; il Ministro dell'università e della ricerca; il Ministro delegato per l'innovazione tecnologica e la transizione digitale; il Ministro delle infrastrutture e della mobilità sostenibili;

il Comitato interministeriale per la cybersicurezza essendo Presieduto dal Presidente del Consiglio non può prevedere anche la contestuale presenza dell'autorità delegata che in quanto tale sarà presente a seguito di eventuale delega del Presidente,

impegna il Governo

a valutare l'opportunità di prevedere che l'Autorità delegata sia presente nel Comitato solo in caso di assenza del Presidente del Consiglio.

---

**G4.103**

MALLEGNI

Il Senato,

in sede di discussione deldecreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale;

premesso che:

l'articolo 4 del decreto istituisce, presso la Presidenza del Consiglio dei ministri, il "Comitato interministeriale per la cybersicurezza" (CIC), organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza;

il comma 3 del citato articolo reca la composizione del Comitato come segue: il Presidente del Consiglio che lo presiede; l'Autorità delegata, ove istituita; il Ministro degli affari esteri e della cooperazione internazionale; il Ministro dell'interno; il Ministro della giustizia; il Ministro della difesa; il Ministro dell'economia e delle finanze; il Ministro dello sviluppo economico; il Ministro della transizione ecologica; il Ministro dell'università e della ricerca; il Ministro delegato per l'innovazione tecnologica e la transizione digitale; il Ministro delle infrastrutture e della mobilità sostenibili;

si ritiene discutibile che la composizione del Comitato non preveda la presenza del Ministro per la pubblica amministrazione essendo la PA uno dei cardini di tutti i sistemi informativi e che detiene tutte le informazioni degli enti locali, dei dipendenti e delle imprese che con essa si interfacciano,

impegna il Governo

a valutare l'opportunità di prevedere che tra i componenti del Comitato interministeriale per la cybersicurezza ci sia anche il Ministro per la Pubblica Amministrazione.

---

**G4.104**

MALLEGNI

Il Senato,

in sede di discussione deldecreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale;

premesso che:

l'articolo 4 del decreto istituisce, presso la Presidenza del Consiglio dei ministri, il "Comitato interministeriale per la cybersicurezza" (CIC), organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza;

il comma 5 del citato articolo dispone che possono partecipare alle sedute del Comitato, su chiamata del Presidente del Consiglio, anche a seguito di loro richiesta, senza diritto di voto: altri componenti del Consiglio dei ministri; altre autorità civili e militari di cui, di volta in volta, ritenga necessaria la presenza in relazione alle questioni da trattare,

il comitato interministeriale ha caratura politica e decide in tal senso. Le autorità civili e militari sono semplicemente elementi di consulenza e saranno chiamati come tali quando necessario. Prevederli per legge nel comitato, seppur senza il diritto di voto, non ha alcun senso se non quello di voler imporre un controllo sul decisore politico,

impegna il Governo:

a valutare la possibilità di espungere la norma di cui al comma 5 richiamato in premessa.

---

**G4.105**

MALLEGNI

Il Senato,

in sede di discussione deldecreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'archi-

tettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale;

premesso che:

l'articolo 4 del decreto istituisce, presso la Presidenza del Consiglio dei ministri, il "Comitato interministeriale per la cybersicurezza" (CIC), organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza;

il comma 6 dello stesso articolo trasferisce al Comitato interministeriale per la cibersicurezza le funzioni già attribuite al Comitato interministeriale per la sicurezza della Repubblica (CISR) dal decreto-legge 105/2019 (DL perimetro) e dai relativi provvedimenti attuativi, fatta eccezione per quelle previste dall'articolo 5 del medesimo decreto-legge 105/2019;

a parere dello scrivente quanto contenuto nel comma 6 andrebbe a svuotare di funzioni il CISR che si occupa di tutta la sicurezza della Repubblica e non solo di quella relativa alla cybersicurezza,

impegna il Governo:

a valutare la possibilità di prevedere la soppressione del citato comma 6.

---

## Art. 5

**G5.100**
MALLEGNI

Il Senato,

in sede di discussione deldecreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale;

premesso che:

l'articolo 5 del decreto reca l'istituzione dell' "Agenzia per la cibersicurezza nazionale" a tutela degli interessi nazionali nel campo della cibersicurezza, con sede in Roma, strumentale all'esercizio delle competenze che il decreto-legge assegna al Presidente del Consiglio dei ministri e all'Autorità delegata, ove istituita ai sensi dell'articolo 5, comma 2), e svolge in particolare le funzioni e i compiti individuati ai sensi del successivo articolo 7;

il comma 2 dell'articolo 5 stabilisce che l'Agenzia ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, nei limiti di quanto previsto dal decreto in oggetto, mentre al comma 3 dispone che il direttore generale e il vice direttore generale hanno la durata massima di 4 anni e possono essere rinnovati per un massimo di ulteriori 4 anni;

il comma 6 precisa che il Copasir "può chiedere l'audizione" del direttore generale dell'Agenzia su questioni di propria competenza, ai sensi di quanto previsto dall'articolo 31, comma 3, della legge 3 agosto 2007, n. 124;

sarebbe opportuno prevedere che il Copasir ottenga (oltre a chiedere) l'audizione del direttore generale dell'Agenzia, posto che qualunque Commissione parlamentare, legata ai Ministeri facenti parte del Comitato interministeriale, può chiedere ed ottenere quindi l'Audizione dello stesso,

impegna il Governo:

a valutare la possibilità di adottare misure volte:

1) riguardo all'autonomia regolamentare attribuita all'Agenzia per la cibersicurezza nazionale, a prevedere che ogni modifica regolamentare, patrimoniale e organizzativa della medesima Agenzia sia approvata con decreto del Presidente del Consiglio dei Ministri, in linea con quanto previsto dall'articolo 6, comma 3;

2) a espungere la possibilità del rinnovo dell'incarico del direttore generale e del vice direttore generale;

3) a prevedere che non possa essere nominato ai vertici dell'Agenzia chi ha svolto funzioni di Governo almeno per i 3 anni successivi all'incarico;

4) a espungere la previsione in base alla quale il direttore generale dell'Agenzia sia il diretto referente anche dell'Autorità delegata ove istituita;

5) a prevedere che il COPASIR ottenga (e non solo chieda) l'audizione del direttore generale dell'Agenzia su questioni di propria competenza.

---

## Art. 6

**G6.100**

MALLEGNI

Il Senato,

in sede di discussione deldecreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'archi-

tettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale;

premesso che:

l'articolo 6 del decreto reca misure relative all'organizzazione dell'Agenzia per la cibersicurezza nazionale;

il comma 3 dispone che il regolamento di organizzazione e funzionamento dell'Agenzia è adottato, entro 120 giorni dalla data di entrata in vigore della legge di conversione del decreto-legge in esame con decreto del Presidente del Consiglio, di concerto con il Ministro dell'economia e delle finanze, previo parere delle competenti Commissioni parlamentari competenti per materia e per i profili finanziari di competenza, del Copasire, sentito il CIC,

impegna il Governo:

a valutare la possibilità di prevedere riguardo all'adozione del regolamento citato, anche il concerto del Ministro della pubblica amministrazione.

---

## Art. 7

**G7.100**
MARILOTTI

Il Senato della Repubblica,

in sede di esame del disegno di legge n. 2336,

visto che l'articolo 7 del relativo decreto-legge fa salvo quanto previsto dal regolamento adottato ai sensi della legge n. 124 del 2007 sul "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto" (cfr. il suo articolo 4, comma 3, lettera l) ),

considerato che l'articolo 4 comma 1 lettera *g)* del Decreto del Presidente del Consiglio dei Ministri n. 5 del 6 novembre 2015 (recante "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva", non ha sin qui ricevuto attuazione in ordine alla promozione di "livelli di sicurezza delle informazioni presso gli organi parlamentari, costituzionali e di rilievo costituzionale",

stante la mole di oltre centomila pagine classificate, presente nell'archivio della Commissione parlamentare d'inchiesta sul terrorismo in Italia e sulle cause della mancata individuazione dei responsabili delle stragi, di cui alle leggi 17 maggio 1988, n. 172, 31 gennaio 1990, n. 12, 28 giugno 1991, n.

215, 13 dicembre 1991, n. 327, 23 dicembre 1992, n. 499, 19 dicembre 1995, n. 538, 20 dicembre 1996, n. 646 e 25 luglio 1997, n. 243, che - anche in ragione dei differenti criteri di inventariazione - rende pressoché impossibile verificare quante e quali pagine coincidano con quelle declassificate ai sensi delle direttive del Presidente del consiglio 8 aprile 2008, 22 aprile 2014 e 2 agosto 2021 e quante siano copie di atti o documenti ancora conservati sotto classifica ai sensi dello speciale regolamento di attuazione adottato ai sensi dell'articolo 10 della legge 3 agosto 2007, n. 124,

impegna il Governo

ad autorizzare, con le cautele di sicurezza informatica più opportune, l'applicazione di un programma di riconoscimento visuale sugli atti citati in premessa, allo scopo di escludere discrasie nell'accessibilità e nella consultabilità dei medesimi atti a seconda che siano presenti nell'Archivio centrale dello Stato, nell'Archivio riservato della Presidenza del consiglio ovvero negli archivi storici del Parlamento.

---

**G7.101**

RAUTI, MALAN

Il Senato,

premesso che:

la definizione della architettura di sicurezza cibernetica si innesta nel contesto istituzionale disciplinato principalmente dal D.Lgs. 65/2018 e dal D.L. 105/2019;

la strategia nazionale di sicurezza cibernetica è un documento previsto dal D.Lgs. 65/2018, di attuazione della direttiva NIS. Ai sensi dell'articolo 6 previgente, il Presidente del Consiglio, previo parere del CISR, adotta la strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale che reca, fra gli altri punti i programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi;

impegna il governo:

a valutare l'opportunità di garantire, nel perimetro delle funzioni dell'Agenzia, la costituzione di aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione ed il reclutamento di personale nei settori avanzati dello sviluppo della cybersicurezza, può inoltre promuovere e finanziare studi di fattibilità e analisi valutative finalizzati a tale scopo.

---

**G7.102**
RAUTI, MALAN

Il Senato,

premesso che:

per gli acquisiti ICT della pubblica amministrazione, nel Piano Nazionale di Ripresa e Resilienza, nella riforma 1.1: ICT - M1C1 - Digitalizzazione, innovazione e sicurezza nella PA, sono previste misure volte a semplificare e velocizzare le procedure mediante una "White List" di fornitori certificati, un percorso accelerato, "Fast Track", una comparazione delle offerte veloce e intuitiva;
sarebbe opportuno attribuire all'Agenzia il compito di indicare le specifiche prescrizioni di sicurezza, da aggiornare regolarmente, per un sistema preliminare di qualificazione e certificazione atto a consentire alle stazioni appaltanti di attribuire agli operatori economici, previa verifica tecnica e regolamentare, una specifica attestazione per la partecipazione alle gare;
impegna il governo:

a valutare l'opportunità, compatibilmente con gli equilibri di finanza pubblica, di adottare iniziative volte all'introduzione, nell'ambito delle funzioni dell'Agenzia di cui al presente decreto, di un sistema volto a definire specifiche prescrizioni di sicurezza, aggiornate regolarmente, anche nell'ambito di un sistema preliminare di qualificazione, ai fini del rilascio agli operatori economici di una specifica attestazione per la partecipazione alle gare della pubblica amministrazione.

---

**G7.103**
RAUTI, MALAN

Il Senato,

premesso che:

l'unificazione delle attività sia normative che di controllo e certificazione nell'ambito della cybersicurezza sotto un'unica autorità, ma con il contributo di conoscenza di dominio delle Autorità di settore, è un oggettivo beneficio sistemico, riduce gli impatti sugli operatori economici e crea uniformità - nel rispetto delle specificità di settore - tra tutti i protagonisti della filiera della resilienza nazionale, rendendo al tempo stesso efficace il processo di rafforzamento del presidio cyber e sostenibili i costi, per effetto delle economie di scala e l'auspicato riferimento a norme di standardizzazione generalmente riconosciute;

una modifica che appare per l'esistenza attuale di una pluralità di soggetti, individuati prevalentemente dalla normativa europea, chiamati a svolgere funzioni di verifica, certificazione, asseverazione dei livelli di sicurezza delle informazioni. La proliferazione di enti di controllo, appartenenti a diversi dicasteri, oltre ad essere antieconomico, determina la stratificazione di attività che potrebbero essere tra di loro contraddittorie e con effetti di disorientamento delle entità soggette a differenti normative;

impegna il governo:

a valutare l'opportunità di adottare iniziative, anche di carattere normativo, volte a razionalizzare ulteriormente le funzioni in materia di cybersicurezza previste dalla normativa nazionale ed europea, con particolare riguardo ai processi di verifica di conformità, ispezione, audit o processi analoghi di verifica, valorizzando il ruolo di coordinamento in materia, previsto in capo all'Agenzia dall'articolo 7, comma 1, lettera a), del decreto in esame.

---

**G7.104**

RAUTI, MALAN

Il Senato,

premesso che:

la minaccia cibernetica è in aumento qualitativo e quantitativo, specialmente verso le pubbliche amministrazioni;

l'impatto del Piano Nazionale di Ripresa e Resilienza nella digitalizzazione della PA sarà ampio, con rischi in aumento esponenziale;

il PNRR, infatti, prevede un programma di digitalizzazione della Pubblica Amministrazione che sia basato su efficacia, velocità e sicurezza ai cittadini e alle imprese nella fruizione dei servizi, pertanto infrastrutture, interoperabilità, piattaforme e servizi, e cybersecurity;

i dati della Polizia Postale evidenziano un aumento, nel 2020, del 353% degli attacchi rispetto l'anno precedente;

in questo raggruppiamo sia gli attacchi diretti alle grandi infrastrutture erogatrici di servizi essenziali (approvvigionamento idrico ed energetico, pubblica amministrazione, sanità, comunicazione, trasporti, finanza sistemica), che gli attacchi apparentemente isolati (diretti a singoli enti, imprese o cittadini);

l'emergenza Covid-19, in particolare, ha costituito un'ulteriore occasione per strutturare e dirigere attacchi ad ampio spettro. Nello specifico, alcune delle più rilevanti infrastrutture sanitarie impegnate nel trattamento dei pazienti "Covid" sono state oggetto di campagne di cyber-estorsione volte alla veicolazione all'interno dei sistemi ospedalieri di sofisticati ransomware a

fronte di richieste di pagamento del prezzo estorsivo, per lo più in cryptovalute (es. Bitcoin). Il sistema sanitario e della ricerca è stato inoltre bersaglio di diversi attacchi APT, con lo scopo della esfiltrazione di informazioni riservate riguardanti lo stato di avanzamento della pandemia e l'elaborazione di misure di contrasto, specie con riguardo all'approntamento di vaccini e terapie anti-Covid;

impegna il governo:

a valutare, compatibilmente con gli equilibri di finanza pubblica, l'opportunità di adottare iniziative volte all'individuazione, nell'ambito dell'Agenzia di una struttura di coordinamento per la cybersicurezza che possa fungere da raccordo per le istanze delle singole amministrazioni in questo settore.

---

**G7.105**

GARRUTI, PERILLI, SANTANGELO, TONINELLI

Il Senato,

in sede di conversione in legge, con modificazioni, del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale (AS 2336);

premesso che:

il presente decreto istituisce l'Agenzia per la cybersicurezza nazionale a tutela degli interessi nazionali nel campo della cybersicurezza, e all'articolo 7 ne identifica le specifiche funzioni;

in particolare la lettera m-*bis*) del comma 1 prevede che l'agenzia assuma le iniziative idonee a valorizzare la crittografia come strumento di cybersicurezza, anche attraverso un'apposita sezione dedicata nell'ambito della strategia nazionale. In particolare, l'Agenzia attiva ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali;

considerato che:

in considerazione dell'accresciuta esposizione alle minacce cibernetiche è emersa negli anni la necessità di sviluppare, in tempi brevi, idonei e sempre più stringenti meccanismi di tutela. Tale esigenza è aumentata negli ultimi anni anche alla luce delle misure volte a garantire infrastrutture *cloud* sicure e centri dati con elevati *standard* di qualità nella direzione di una crescente interoperabilità e condivisione delle informazioni;

in base ad una analisi del trend degli attacchi informatici perpetrati a danno della PA e delle imprese, si evidenzia una forte debolezza del sistema informatico paese. Purtroppo sono mancati negli anni investimenti e competenze per proteggere gli asset digitali e immateriali. Mancano, inoltre, competenze specifiche ed una reale consapevolezza del problema da parte della dirigenza: è palese la divaricazione tra requisiti di prevenzione e precauzione previsti dalle normative e la messa in opera totalmente insufficiente. Questo genera anche frustrazione nelle aspettative di cittadini nei confronti della PA, specialmente quelli più consapevoli che non vedono messe in opera le previsioni di legge destinate a proteggerli;

oggi il sistema informatico paese è vulnerabile e bisogna avere elevate competenze, professionalità e istituire percorsi che già dalla scuola comincino a formare le future generazioni;

gli ultimi sviluppi normativi hanno cercato di predisporre un quadro idoneo a rafforzare il contesto della cybersecurity a livello europeo e nazionale.

A livello di Unione europea la direttiva (UE) 2016/1148 del 6 luglio 2016 reca misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. direttiva NIS - *Network and Information Security*") al fine di conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea;

la direttiva è stata recepita nell'ordinamento italiano con il decreto legislativo n. 65 del 18 maggio 2018, che detta quindi la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS;

successivamente, il decreto-legge n. 105 del 2019 è stato adottato al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi;

la sicurezza cibernetica costituisce uno degli interventi previsti dal Piano nazionale di ripresa e resilienza (PNRR) trasmesso dal Governo alla Commissione europea il 30 aprile 2021 e definitivamente approvato il 13 luglio 2021;

considerato, inoltre, che:

in attuazione del decreto legge 105 del 2019 è stato esaminato nel marzo 2021 dal Parlamento uno schema di decreto del Presidente del Consiglio dei ministri recante regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b) del decreto-legge 21 settembre 2019, n. 105, con-

vertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza;

già in tal sede, durante l'esame della commissione Affari Costituzionali del Senato, era emerso come l'algoritmo di cifratura nazionale sia una soluzione completamente inapplicabile nel contesto del funzionamento della rete internet, che funziona sulla base di protocolli standardizzati e condivisi a livello globale. A seguito di una ulteriore interlocuzione con il Dipartimento delle informazioni per la sicurezza (DIS), per il tramite del Ministro dei rapporti con il Parlamento, è infatti emerso che la misura non è applicabile sotto il profilo tecnico e informatico;

la sicurezza end-to-end viene implementata rafforzando la sicurezza dei protocolli esistenti in modo che siano sempre più resistenti agli attacchi cibernetici e non introducendo ulteriori brecce di vulnerabilità né proposte altamente costose e non facilmente integrabili nell'operatività di internet;

l'algoritmo utilizzato nelle comunicazioni crittografate *end-to-end*, necessario per la decrittazione e ricezione dei dati trasmessi, deve necessariamente rispettare standard internazionali ed essere utilizzabile a livello globale, per cui non può avere una connotazione solo nazionale che, tra l'altro, comporterebbe maggiori rischi sotto il profilo della sicurezza;

impegna il Governo:

a prevedere nell'ambito della strategia nazionale che si incentivi la formazione di profili professionali in numero adeguato alle esigenze di protezione informatica del Paese e di ricercatori che possano ulteriormente contribuire a migliorare lo sviluppo della ricerca di base in ambito crittografico e di tecnologie di sicurezza informatica;

a prevedere che l'Agenzia per la cybersicurezza nazionale favorisca la ricerca scientifica in vista di algoritmi che necessariamente si possano inserire negli standard internazionali ed essere utilizzabili a livello globale, favorendo, nell'azione di rafforzamento dell'autonomia industriale e tecnologica dell'Italia, lo sviluppo di algoritmi brevettabili o nuove capacità crittografiche nazionali.

## Art. 10

**G10.100**
RAUTI, MALAN

Il Senato,

il testo in esame reca la conversione in legge del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di *cyber*sicurezza, definizione dell'architettura nazionale di *cyber*sicurezza ed istituzione dell'Agenzia per la *cyber*sicurezza nazionale;

data la crescente e progressiva interdipendenza delle Pubbliche Amministrazioni e dei settori strategici nazionali con le infrastrutture materiali ed immateriali di rete sono in costante aumento i profili di rischio a danno della sicurezza e della capacità di erogazione dei servizi delle amministrazioni nazionali e locali;

considerato che il *digital divide* colpisce tuttora buona parte del Paese ed esiste una vera e propria sperequazione a detrimento delle aree interne, montane e rurali, è chiaro che determinate amministrazioni e categorie di cittadini sono più vulnerabili alle ripercussioni degli attacchi cibernetici nonché a *data breach* che possano mettere a repentaglio i propri dati sensibili;

il testo in esame rappresenta un riconoscimento fondamentale delle nuove esigenze e profili di rischio rappresentati dalle interconnessioni digitali, e pertanto non è più procrastinabile una azione ad ampio raggio da parte del Governo per mettere in sicurezza i sistemi IT delle amministrazioni pubbliche,

impegna il Governo a:

valutare la possibilità di garantire risorse per l'ammodernamento informatico dei sistemi IT di tutti i comparti della Pubblica Amministrazione, con particolare riguardo per gli enti territoriali e le amministrazioni situate nelle aree interne, in pieno processo di superamento del *digital* divide, per superare l'obsolescenza dei sistemi attuali che adoperano tecnologie facilmente aggredibili dall'esterno.

**G10.101**

RAUTI, MALAN

Il Senato,

premesso che:

Nelle premesse del Decreto si rintraccia nel PNRR una delle ragioni per cui si dà corso alla nascita dell'Agenzia per la Cybersicurezza Nazionale;

Gli investimenti in digitalizzazione del PNRR consistono in più di un terzo delle risorse messe in campo dal dispositivo;

Il PNRR prevede quindi, innanzitutto, un programma di digitalizzazione della Pubblica Amministrazione che offra efficacia, velocità e sicurezza ai cittadini e alle imprese nella fruizione dei servizi, pertanto infrastrutture, interoperabilità, piattaforme e servizi, e cyber security;

Inoltre, verranno inserite "misure propedeutiche alla piena realizzazione delle riforme chiave delle Amministrazioni Centrali, quali lo sviluppo e l'acquisizione di (nuove) competenze per il personale della PA (anche con il miglioramento dei processi di upskilling e di aggiornamento delle competenze stesse) e una significativa semplificazione/sburocratizzazione delle procedure chiave, incluso uno sforzo dedicato al Ministero della Giustizia per lo smaltimento del backlog di pratiche";

In questo modo, la Pubblica Amministrazione subirà in positivo una sorta di rivoluzione per quanto riguarda le dotazioni tecnologiche, il personale e le infrastrutture, così come nella sua stessa organizzazione e nelle procedure interne e orientate al cittadino;

Il capitolo dedicato specificatamente alla cyber security all'interno del documento redatto dal governo riguarda un settore limitato della security. Oltre a un budget piuttosto sottodimensionato (solo 623 milioni di euro) il punto si concentra sugli aspetti di sicurezza informatica legati a quelli che si possono definire "gli interessi nazionali", cioè le infrastrutture critiche, le forze di polizia e i nuovi enti (forse ne sono previsti anche troppi) cui verranno affidati compiti come l'assessment di software e hardware;

Per quanto riguarda il settore pubblico, gli unici riferimenti specifici alla cyber security si trovano nel capitolo dedicato alla Pubblica Amministrazione, mentre per il settore della cultura, si parla soltanto di interventi "facendo leva sulle nuove tecnologie per offrire nuovi servizi e migliorare l'accesso alle risorse turistiche/culturali";

La digitalizzazione, infatti, è un obiettivo trasversale del PNRR, comprendente, in particolare, le Missioni 2,3,6, dalla scuola, all'economia circolare, alla connessione dei luoghi sportivi, alla ricerca, alla telemedicina;

La pandemia, infatti, ha dato spinta alla dematerializzazione del segmento fisico delle attività umane;

Nell'anno della pandemia, secondo il Rapporto Clusit 2021, sono stati infatti 1.871 gli attacchi gravi di dominio pubblico, con un incremento del 12% rispetto al 2019. In aumento, in particolare, gli eventi di spionaggio

cyber. Questi attacchi hanno avuto un impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica. Ciò significa che, in media, sono stati registrati ben 156 attacchi gravi al mese, il valore più elevato mai registrato ad oggi (erano 139 nel 2019), con il primato negativo che spetta al mese di dicembre, in cui sono stati rilevati ben 200 attacchi gravi;

Si conferma, quindi, il trend di crescita costante che, dal 2017 ad oggi, ha fatto segnare un aumento degli attacchi gravi del 66%;

Secondo i dati in possesso della Polizia Postale, gli attacchi informatici in Italia sono aumentati del 246% solo nel 2020;

Nell'anno segnato dall'emergenza sanitaria, non stupisce che numerosi tentativi di furto di dati abbiano riguardato anche informazioni in ambito sanitario: l'Agenzia Europea del Farmaco ha subito un cyber attacco tramite cui sono stati violati documenti sul vaccino Pfizer, mentre un gruppo di hacker nordcoreani ha effettuato una serie di tentativi di intrusione nei sistemi della casa farmaceutica AstraZeneca durante le fasi di sperimentazione del vaccino;

impegna il governo:

a valutare l'opportunità, compatibilmente con gli equilibri di finanza pubblica, di adottare iniziative, anche di carattere normativo, a garantire l'istituzione di una zona economica speciale per le aziende della sicurezza cibernetica, garantendo meccanismi fiscali agevolati, anche al fine di garantire la sovranità digitale e sostenere la politica industriale nazionale.

---

**G10.102**

RAUTI, MALAN

Il Senato,

premesso che:

Il provvedimento in esame reca misure urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale;

La minaccia cibernetica è in aumento qualitativo e quantitativo, specialmente verso le pubbliche amministrazioni;

L'impatto del Piano Nazionale di Ripresa e Resilienza nella digitalizzazione della PA sarà ampio, con rischi in aumento esponenziale;

Il PNRR, infatti, prevede un programma di digitalizzazione della Pubblica Amministrazione che sia basato su efficacia, velocità e sicurezza ai cittadini e alle imprese nella fruizione dei servizi, pertanto infrastrutture, interoperabilità, piattaforme e servizi, e cybersecurity;

I dati della Polizia Postale evidenziano un aumento, nel 2020, del 353% degli attacchi rispetto l'anno precedente;

In questo raggruppiamo sia gli attacchi diretti alle grandi infrastrutture erogatrici di servizi essenziali (approvvigionamento idrico ed energetico, pubblica amministrazione, sanità, comunicazione, trasporti, finanza sistemica), che gli attacchi apparentemente isolati (diretti a singoli enti, imprese o cittadini);

L'emergenza Covid-19, in particolare, ha costituito un'ulteriore occasione per strutturare e dirigere attacchi ad ampio spettro. Nello specifico, alcune delle più rilevanti infrastrutture sanitarie impegnate nel trattamento dei pazienti "Covid" sono state oggetto di campagne di cyber-estorsione volte alla veicolazione all'interno dei sistemi ospedalieri di sofisticati ransomware a fronte di richieste di pagamento del prezzo estorsivo, per lo più in cryptovalute (es. Bitcoin). Il sistema sanitario e della ricerca è stato inoltre bersaglio di diversi attacchi APT, con lo scopo della esfiltrazione di informazioni riservate riguardanti lo stato di avanzamento della pandemia e l'elaborazione di misure di contrasto, specie con riguardo all'approntamento di vaccini e terapie anti-Covid;

impegna il governo:

a valutare l'opportunità, compatibilmente con gli equilibri di finanza pubblica, di prevedere l'aumento delle agevolazioni fiscali o incentivi per l'acquisto di software, sistemi, piattaforme e applicazioni per la protezione di dati, reti, macchine, programmi e impianti da attacchi, danni e accessi non autorizzati.

---

**G10.103**

RAUTI, MALAN

Il Senato,

premesso che:

il testo in esame reca la conversione in legge del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di *cyber*sicurezza, definizione dell'architettura nazionale di *cyber*sicurezza ed istituzione dell'Agenzia per la *cyber*sicurezza nazionale;

nella fattispecie il testo in esame evidenzia l'importanza per lo Stato italiano di dotarsi delle necessarie infrastrutture materiali ed immateriali per il potenziamento dei profili di sicurezza del Paese in un'ottica cibernetica ed alla luce della crescente interdipendenza degli apparati strategici nazionali con l'utilizzo della rete;

è interesse nazionale improcrastinabile la conversione degli apparati produttivi ad una logica di interconnessione strategica nell'ambito ciber-

netico e digitale, anche dal punto di vista delle forniture per le imprese operanti nei settori strategici e nella Pubblica Amministrazione;

data la crescente importanza di capacità gestionale della sicurezza digitale e cibernetica, è necessario che il sistema produttivo nazionale effettui il prima possibile la transizione verso ottiche di sicurezza digitale,

impegna il Governo a:

valutare l'opportunità di prevedere l'obbligo, per imprese operanti in settori strategici e Pubblica Amministrazione, di adottare strumenti, prodotti e tecnologie "*hack proof"* e, nelle circostanze più delicate, di certificazioni "*accountable*" (es. ISO 27001), anche prevedendo incentivi economici per la dotazione dei predetti sistemi.

---

**G10.104**

RAUTI, MALAN

Il Senato,

premesso che:

il provvedimento in esame tratta il tema della cybersicurezza, una materia quanto mai fondamentale al fine di garantire la tutela dell'interesse nazionale e del diritto alla riservatezza e corretta tutela dei dati dei cittadini;

con il decreto-legge 82/2021 è stata istituita l'Agenzia Nazionale per la Cybersicurezza, l'Autorità alla quale spettano compiti di controllo e prevenzione in termini di attacco di natura cibernetica a tutela degli interessi nazionali;

l'interesse superiore della sicurezza necessita di una sempre maggiore collaborazione pubblico-privato al fine di garantire un sistema resiliente e capace di affrontare le sfide tecnologiche nonché le minacce cyber;

con il Regolamento (CE) n. 460/2004 del 10 marzo 2004 è stata istituita l'ENISA (European Union Agency for Network and Information Security), con la quale si intende stimolare un'ampia cooperazione tra gli attori del settore pubblico e privato;

è sempre più rilevante introdurre dei criteri di valutazione oggettivi al fine di poter perimetrare il quadro delle aziende capaci di soddisfare i requisiti come certificazioni, protocolli e regolamenti che garantiscono il rispetto dei più alti standard in materia di sicurezza cibernetica;

L'FBI e la Cybersecurity and Infrastrutture Security Agency (CISA) hanno rivelato il 20 luglio con un comunicato congiunto che diverse società statunitensi di gas naturale e oleodotti sono state violate con successo da hacker cinesi per due anni a partire dal 2011 ; le sopracitate agenzie hanno evidenziato che 13 società sono state violate con successo, tre sono stati de-

scritti come «quasi incidenti» e altre otto sono state soggette a una «profondità sconosciuta di intrusione» che CISA e FBI hanno attribuito ad hacker sponsorizzati dallo stato cinese valutando che gli attacchi miravano probabilmente a sviluppare ulteriormente le capacità cyber offensive della Cina;

l'evoluzione tecnologica ha portato alla digitalizzazione di ogni infrastruttura strategica alla penetrazione dei sistemi da parte di terze parti al fine della loro manomissione o per sottrarre informazioni riservatissime dall'alto valore commerciale o competitivo,

impegna il Governo

a valutare l'opportunità, compatibilmente con gli equilibri di finanza pubblica, di prevedere un sistema di certificazione tra le aziende private che consenta di creare un elenco di operatori in possesso di determinati requisiti di sicurezza, che possano partecipare alle gare pubbliche in ambito digitale.

---

**G10.105**

BINETTI

Il Senato,

in sede di discussione deldecreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.

premesso che:

l'Unione Europea considera il processo di digitalizzazione come strumento essenziale a servizio della sanità, per questo si considerano inderogabili le strategie necessarie per superare le "barriere" che si oppongono ad una piena trasformazione digitale e allo sfruttamento dei dati che ne derivano in termini di interoperabilità, comprese le norme etico-giuridiche, che riguardano la governance, la sicurezza informatica, e i requisiti tecnici, in conformità alle norme sulla protezione dei dati personali (Directive 95/46/EC (General Data Protection Regulation));

la transizione digitale è oggi il presupposto per consentire alle organizzazioni che compongono il sistema sanitario di raggiungere gli obiettivi del Piano Oncologico Nazionale, per questo motivo la transizione digitale assume rilevanza strategica e trasversale rispetto agli altri temi trattati dal Piano;

lo sforzo è quello di realizzare l'ecosistema sanitario con una visione strategica, sistemica e integrata, che consenta l'interoperabilità dei sistemi ICT, riducendo il rischio di disallineamenti locali. La crisi, determinata dalla pandemia, ha evidenziato la necessità di diffondere nuovi strumenti digitali e di sanità elettronica;

per sanità digitale si intendono tutte le tecnologie dell'informazione e della comunicazione (ICT) necessarie per far funzionare il sistema sanitario: dalla ricetta elettronica alla telemedicina e teleassistenza, al supporto per gli studi epidemiologici e di ricerca clinica. Si potranno inoltre effettuare a domicilio, o in prossimità del paziente, una serie di attività diagnostiche; permettere un monitoraggio continuo a distanza; ridurre gli accessi alle strutture ospedaliere e i ricoveri senza penalizzare l'assistenza sanitaria;

condizione necessaria per traguardare al 2026 il nuovo ecosistema del SSN è poter disporre di una governance nazionale del sistema digitale nell'ambito del SSN, che operi in condizione di massima sicurezza, sia per quanto riguarda i dati del paziente e la sua privacy, che per quanto si riferisce all'architettura complessiva del sistema digitale;

il processo di digitalizzazione del sistema sanitario deve quindi identificare con chiarezza obiettivi e strategie per valutare di quante e quali risorse ha bisogno. Prima però deve prendere atto delle attuali difficoltà, chepossono essere così sintetizzate:

- le infrastrutture informatiche e digitali non sono uniformemente sviluppate e disponibili sul territorio; i flussi informativi, che dovrebbero alimentare il sistema digitale, ad oggi non sono ancora chiaramente e uniformemente regolamentati ed interoperabili;

- il fascicolo sanitario elettronico non è ovunque operativo e spesso non è alimentato da tutte le strutture sanitarie pubbliche o private convenzionate, talora per motivi addotti di protezione dei dati personali e l'accesso ai dati per finalità cliniche e di ricerca a programmazione sanitaria è ancora limitato;

- la standardizzazione nella raccolta delle informazioni è ancora carente e poco condivisa sul territorio, con regioni che raccolgono ancora dati con criteri e sistemi di classificazione differenti tra loro;

- l'alfabetizzazione informatica di pazienti, caregivers e anche di molti operatori sanitari è scarsa e disomogenea;

Gli obiettivi, per cui si chiede al Ministero della transizione digitale di prestare particolare attenzione, sono:

1. Implementazione del Fascicolo Sanitario Elettronico (FSE) e della cartella oncologica informatizzata e della sua interoperabilità, ai fini di migliorare le attività di prevenzione primaria, la gestione degli screening e la presa in carico del paziente dal momento della diagnosi alla fase di terapia, con un monitoraggio a breve, medio a lungo termine.

2. Potenziamento della Telemedicina, Teleconsulto clinico/patologico sia nell'ambito delle Reti Oncologiche Regionali che nell'ambito della Rete Nazionale Tumori Rari (con meccanismi di remunerazione delle prestazioni), con Telemonitoraggio del percorso di cura e degli effetti collaterali per migliorare la qualità delle cure, l'aderenza terapeutica e una migliore qualità della vita.

3. Raccolta e analisi sistematica dei dati sanitari per finalità di ricerca clinica e epidemiologica e per la programmazione sanitaria al fine di ottimizzare l'organizzazione sanitaria, con riduzione della ripetizione degli esami e delle visite e una migliore continuità ospedale-territorio.

4. Sviluppo di infrastrutture digitali quali principali abilitatori che permetteranno ai cittadini di sfruttare le enormi potenzialità delle tecnologie di nuova generazione. Il 5G migliorerà la velocità di connessione e consentirà anche lo sviluppo di applicazioni che richiedono bassa latenza e alta affidabilità.

in considerazione degli obiettivi indicati si propongono le seguenti Linee strategiche:

1. garantire il processo di transizione digitale e la piena attivazione del FSE; della Cartella Clinica informatizzata; e la costituzione delle Reti di Telemedicina e Telepatologia a livello regionale e nazionale;

2. garantire un accesso regolamentato alle informazioni contenute nel FSE e nella Cartella Clinica informatizzata sia per finalità cliniche che socio-assistenziali a servizio del paziente, sia per finalità di ricerca, sia per la programmazione dei servizi socio-sanitari e assistenziali;

3. realizzare la smart card in cui si riassume la storia clinica dei pazienti per facilitarne il follow-up. La tessera, personalizzata e volontaria, migliorerà la comunicazione e il coordinamento tra medico e paziente, in accordo con le iniziative "Faro 8 fondi del programma EU4Health"

4. ultimare i processi di digitalizzazione per la tracciabilità dei campioni biologici sottoposti ad esami di Anatomia Patologica, come base per la costituzione delle bio-banche oncologiche.

5. implementare le strumentazioni per la produzione del vetrino digitale e definire le normative ministeriali che ne autorizzino l'utilizzo come naturale evoluzione tecnologica dell'Anatomia Patologica, in analogia alla Radiologia.

6. promuovere la creazione di consorzi e dipartimenti virtuali per condividere le risorse di reparti di oncologia pediatrica in attuazione della Rete Nazionale Tumori Rari (RNTR) che si avvale di servizi di telemedicina e teleconsulto, che già lavorano in 3 reti professionali: 1 rete per i tumori rari solidi dell'adulto; 1 rete per l'onco-ematologia; 1 rete per i tumori pediatrici

7. promuovere la formazione digitale degli operatori della sanità e delle associazioni dei malati oncologici, dei pazienti e dei loro caregivers;

per realizzare una transizione tecnologica così ampia e profonda servono risorse adeguate che potrebbero essere attinte da:

1. fondi previsti dal Piano Nazionale di Ripresa e Resilienza (PNRR) del 2021 che prevedono nella Mission 6C2 "Innovazione, ricerca e digitalizzazione del Servizio Sanitario Nazionale interventi strutturali e di innovazione tecnologica per la sanità, specificati nei due punti "Sviluppare una sanita`

pubblica che valorizzi gli investimenti nel sistema salute in termini di risorse umane, digitali, strutturali, strumentali e tecnologici" e "Rafforzare la ricerca scientifica in ambito biomedico e sanitario"

2. fondi previsti dall'EU4Health Programme (EU4H), il programma dell'EU in materia di salute, che individua il cancro come settore trasversale di intervento

3. fondo europeo di sviluppo regionale, Fondo di coesione e Fondo sociale europeo Plus

4. la Commissione ha inoltre presentato una proposta di strumento di sostegno tecnico77 per fornire un sostegno pratico a tutti gli Stati membri dell'UE che esprimano interesse nei confronti di riforme istituzionali, amministrative e a favore della crescita.

5. gli investimenti connessi al cancro da parte di Stati membri ed enti pubblici e privati potrebbero essere mobilitati anche attraverso le garanzie dell'Unione, ad esempio il programma InvestEU. La Commissione europea istituirà un meccanismo di condivisione delle conoscenze per informare gli Stati membri sui diversi meccanismi di finanziamento dell'UE e sulle relative modalità di utilizzo.

6. fondi nazionali e regionali destinati al sostegno delle Startup che operano nel settore del Mhealth;

tutto ciò risulta di particolare interesse dopo i due anni di una pandemia, che non è ancora risolta e che ha visto i malati oncologici spesso trascurati o non adeguatamente presi in carico, con tutte le conseguenze che ciò comporta e con la certezza che la digitalizzazione consapevole del sistema può contribuire a limitare i danni accumulati e convertire il sistema in una realtà più dinamica ed efficiente,

impegna il Governo:

a valutare la possibilità di adottare misure volte a realizzare quanto indicato nelle premesse.

## Art. 11

**G11.100**
MALLEGNI

Il Senato,

in sede di discussione deldecreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale;

premesso che:

l'articolo 11 detta le disposizioni relative al sistema di finanziamento dell'Agenzia e all'autonomia contabile e gestionale della stessa;

il comma 3 prevede che il regolamento di contabilità dell'Agenzia, che ne assicura l'autonomia gestionale e contabile, è adottato con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, su proposta del direttore generale dell'Agenzia, previo parere del COPASIR e sentito il CIC, entro centoventi giorni dalla data di entrata in vigore della legge di conversione del presente decreto, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, e alle norme di contabilità generale dello Stato;

ogni norma e regolamento deve rispondere ai criteri della contabilità generale dello Stato e non devono essere ammesse deroghe,

impegna il Governo:

a valutare la possibilità di prevedere, pur nel rispetto dell'autonomia gestionale e contabile dell'Agenzia, che non si deroghi alle norme di contabilità generale dello Stato.

---

## Art. 12

**G12.100**
MALLEGNI

Il Senato,

in sede di discussione deldecreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'archi-

tettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale;

premesso che:

l'articolo 12 reca la disciplina del personale dell'Agenzia per la cybersicurezza demandando ad un regolamento la definizione dell'ordinamento e del reclutamento del personale, nonché il relativo trattamento economico e previdenziale;

si dispone che tale Regolamento deve assicurare per il personale di ruolo dell'Agenzia un trattamento economico pari a quello in godimento da parte dei dipendenti della Banca d'Italia, in base alla "equiparabilità delle funzioni svolte e del livello di responsabilità rivestito;

inoltre, il Regolamento determina: la possibilità di procedere, oltre che ad assunzioni a tempo indeterminato attraverso modalità concorsuali, ad assunzioni a tempo determinato, con contratti di diritto privato, di soggetti in possesso di alta e particolare specializzazione debitamente documentata, individuati attraverso adeguate modalità selettive, per lo svolgimento di attività assolutamente necessarie all'operatività dell'Agenzia o per specifiche progettualità da portare a termine in un arco di tempo prefissato; la possibilità di avvalersi di un contingente di esperti, non superiore a cinquanta unità, composto da personale collocato fuori ruolo o in posizione di comando o altra analoga posizione, prevista dagli ordinamenti di appartenenza, proveniente da pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, con esclusione del personale docente, educativo, amministrativo, tecnico e ausiliario delle istituzioni scolastiche, ovvero da personale non appartenente alla pubblica amministrazione, in possesso di specifica ed elevata competenza in materia di cybersicurezza e di tecnologie digitali innovative, nello sviluppo e gestione di processi complessi di trasformazione tecnologica e delle correlate iniziative di comunicazione e disseminazione, nonché di significativa esperienza in progetti di trasformazione digitale, ivi compreso lo sviluppo di programmi e piattaforme digitali con diffusione su larga scala. Il regolamento, a tali fini, disciplina la composizione del contingente e il compenso spettante per ciascuna professionalità,

a parere dello scrivente il personale dipendente deve essere assunto tra coloro che in via prioritaria sono già dipendenti dello Stato o in generale della funzione pubblica, con la possibilità di ammesse ulteriori assunzioni esclusivamente attraverso concorso pubblico;

inoltre, per quanto riguarda il trattamento economico, occorrerebbe attribuire al personale dell'Agenzia lo stesso trattamento economico dei dipendenti delle altre Autorità nazionali,

impegna il Governo:

a valutare la possibilità di apportare le opportune modifiche al citato articolo 12, secondo le indicazioni esposte in premessa.

———————