Senato della Repubblica

XVIII LEGISLATURA

Assemblea

RESOCONTO STENOGRAFICO
ALLEGATI

ASSEMBLEA

354ª seduta pubblica

martedì 3 agosto 2021

Presidenza del presidente Alberti Casellati,

indi del vice presidente La Russa

INDICE GENERALE

I N D I C E

N.B. Sigle dei Gruppi parlamentari: Forza Italia Berlusconi Presidente-UDC: FIBP-UDC; Fratelli d'Italia: FdI; Italia Viva-P.S.I.: IV-PSI; Lega-Salvini Premier-Partito Sardo d'Azione: L-SP-PSd'Az; MoVimento 5 Stelle: M5S; Partito Democratico: PD; Per le Autonomie (SVP-PATT, UV): Aut (SVP-PATT, UV); Misto: Misto; Misto-IDEA e CAMBIAMO: Misto-IeC; Misto-Italia dei Valori: Misto-IdV; Misto-l'Alternativa c'è-Lista del Popolo per la Costituzione: Misto-l'A.c'è-LPC; Misto-Liberi e Uguali-Ecosolidali: Misto-LeU-Eco; Misto-Movimento associativo italiani all'estero: Misto-MAIE; Misto-+Europa - Azione: Misto-+Eu-Az; Misto-Potere al Popolo: Misto-PaP.

RESOCONTO STENOGRAFICO

Presidenza del presidente ALBERTI CASELLATI

PRESIDENTE. La seduta è aperta *(ore 16,32).*
Si dia lettura del processo verbale.

MARGIOTTA, *segretario, dà lettura del processo verbale della seduta del 29 luglio.*

PRESIDENTE. Non essendovi osservazioni, il processo verbale è approvato.

Comunicazioni della Presidenza

PRESIDENTE. L'elenco dei senatori in congedo e assenti per incarico ricevuto dal Senato, nonché ulteriori comunicazioni all'Assemblea saranno pubblicati nell'allegato B al Resoconto della seduta odierna.

Sull'ordine dei lavori

PRESIDENTE. Informo l'Assemblea che all'inizio della seduta il Presidente del Gruppo MoVimento 5 Stelle ha fatto pervenire, ai sensi dell'articolo 113, comma 2, del Regolamento, la richiesta di votazione con procedimento elettronico per tutte le votazioni da effettuare nel corso della seduta. La richiesta è accolta ai sensi dell'articolo 113, comma 2, del Regolamento.

Sul centenario della traslazione del Milite ignoto

PRESIDENTE. *(Il Presidente e l'Assemblea si levano in piedi).* Senatori, il prossimo 11 agosto sarà il centesimo anniversario della promulgazione della legge che ha disposto la traslazione all'Altare della Patria della salma del Milite ignoto: un atto solenne voluto dal Parlamento per onorare la memoria dei 651.000 soldati italiani caduti durante la Prima guerra mondiale. Il loro sacrificio è testimonianza di alcune delle pagine più drammatiche della nostra storia: pagine di coraggio, pagine di eroismo e altruismo, di cui sono stati protagonisti i nostri soldati, così come delle loro umane paure, delle angosce e delle frustrazioni che nelle trincee di confine accompagnavano lo scoppio di ogni colpo di artiglieria. Pagine scritte con il sangue di tanti giovani che hanno affrontato gli orrori della guerra e con il dolore di genitori, mogli e figli che non li hanno visti tornare a casa, e a cui troppo spesso è stata perfino negata l'intima pietà di una tomba o di una lapide su cui piangere o deporre un fiore. Nel tempo, le spoglie di quel giovane milite senza nome

sono diventate il simbolo del grande cuore di tutti gli italiani in divisa, che hanno perso la vita in guerra o in missione ovunque nel mondo; donne e uomini di ogni generazione che hanno difeso con orgoglio, incrollabile senso del dovere e instancabile dedizione, la Patria e i suoi valori; valori che oggi sono le fondamenta di una Nazione libera e dialogante.

Un Paese che crede fermamente nella pace come bene comune da proteggere contro ogni forma di violenza o di prevaricazione; un Paese che non dimentica e che, in questo solenne centesimo anniversario, onora i suoi martiri con iniziative meritorie e di valore, come l'idea di riconoscere la cittadinanza onoraria al milite ignoto da parte di tutti i Comuni d'Italia, come il Treno della memoria, che il prossimo 28 ottobre partirà da Aquileia per giungere a Roma il 4 novembre, unendo ancora una volta il Paese in un nuovo viaggio simbolico, sulle orme di quello che un secolo fa portò le spoglie del milite ignoto fino all'Altare della Patria. Soprattutto un Paese che racconta, spiega, tramanda la propria storia alle generazioni di oggi e a quelle di domani, perché si facciano anch'esse messaggere di una memoria che è parte della loro identità culturale, oltre che una guida preziosa per costruire un futuro migliore, perché comprendano davvero l'inestimabile ricchezza di un patrimonio di principi, tutele e garanzie individuali e collettive che è frutto anche di grandi sofferenze e sacrifici di vite umane. Vi ringrazio *(Applausi)*.

Sui gravi incendi che hanno colpito il territorio italiano

D'ALFONSO *(PD)*. Domando di parlare.

PRESIDENTE. Ne ha facoltà.

D'ALFONSO *(PD)*. Signor Presidente, la ringrazio anche per la cortesia istituzionale che ha voluto usarmi.

Intervengo per richiamare l'attenzione di quest'Assemblea e, attraverso di essa, del discorso pubblico della nostra Nazione sul disastro che ha colpito la Regione Abruzzo: una vera e propria strage di alberi che domenica abbiamo purtroppo patito come comunità regionale, a causa di una condotta scellerata di coloro i quali hanno voluto distruggere attraverso il fuoco un patrimonio irripetibile coincidente con il creato.

Mi riferisco a un creato che ci fa pensare, in termini di sentimento, di avvertimento delle coscienze, a quello che lei ha richiamato prima a proposito dell'opera estrema garantita dal Milite ignoto, perché la Patria che evoca il suolo sotto il quale sono sepolti i nostri avi è fatta anche del paesaggio, del creato, di quanto consente memoria individuale e collettiva.

In Abruzzo abbiamo perso qualcosa come 100.000 alberi. Un sacerdote di grande credibilità, monsignor Iannucci di Pescara, ha insegnato a numerose generazioni che gli alberi sono i cittadini che avremmo voluto avere in più. Il Parco D'Avalos, di cinquecento anni di vita, ha perso più di un terzo della sua consistenza, ma sono state colpite anche la pineta dannunziana, quella che ha ispirato la riflessione, il pensiero e le opere di D'Annunzio, così come la Costa dei Trabocchi.

Intervenire in Senato in questo momento serve a richiamare l'attenzione delle istituzioni. Il codice di protezione civile del 2020 prevede che davanti a questi disastri si attivino le procedure per il riconoscimento dell'emergenza nazionale. E ci sono gli elementi per l'emergenza nazionale, dal momento che sono stati rimossi dei pericoli, sono state evacuate persone e famiglie, senza contare tutto quello che ho descritto come perdita ambientale. Se però ci fosse solo l'intervento degli organi statuali governativi, non ripristineremmo il valore del Paese saggio che è evocato dal paesaggio. C'è bisogno anche di fare di più ad opera della cittadinanza, ad opera di coloro i quali hanno molto, anche sul piano della ricchezza. Infatti ci vorranno almeno quindici anni per ripristinare quei 100.000 alberi per le giovani generazioni che vorranno rivendicare il diritto alla veduta della bellezza. Serviranno norme per scoraggiare questi delinquenti che attraverso il fuoco hanno distrutto il Creato; serviranno sanzioni, risorse per fare in modo che i progetti di carattere ambientale dispongano anche di colonnine che distribuiscono acqua, estintori su misura del rischio, attraverso il principio di precauzione.

Il messaggio ulteriore che vorrei mandare attraverso questo intervento è che dobbiamo fare in modo che le vicende vengano evitate a monte e non a valle, perché intervenire a valle richiede risorse in più, richiede ed impone una perdita di diritti delle giovani generazioni.

Signor Presidente, vorrei tanto che la cura e la premura dei Ministeri competenti mettessero in evidenza come la provvista finanziaria deve essere su misura dei valori che abbiamo nelle terre alte delle nostre Regioni.

La ringrazio per avermi consentito di fare questo intervento. *(Applausi)*.

PAGANO *(FIBP-UDC)*. Domando di parlare.

PRESIDENTE. Ne ha facoltà.

PAGANO *(FIBP-UDC)*. Signor Presidente, anch'io mi sento in dovere di intervenire qui, nella Camera alta del Parlamento. Mi rivolgo a lei, cara Presidente, che è stata a Pescara soltanto pochi giorni fa ed è stata proprio a pochi metri dalla pineta D'Avalos, denominata dannunziana in quanto il Vate ebbe a comporre una poesia, «La pioggia nel pineto», che evocava esattamente quella pineta. È proprio questo il problema: l'incendio è scoppiato di fatto in città ed è stato forse questo l'elemento drammatico della notizia dell'incendio di Pescara rispetto ai tanti incendi che hanno devastato i boschi e le foreste in tutta Italia, rispetto ai quali ovviamente esprimiamo vicinanza, perché perdere patrimonio boschivo, perdere foreste significa perdere un pezzo della nostra vita e della nostra storia. Pescara però all'interno della città ha non solo un parco, non solo un polmone verde, ma un pezzo della propria storia. Per i pescaresi aver perso più di un terzo del patrimonio forestale di un parco, che divenne di fatto più di dieci anni fa una riserva naturale, ha significato perdere un pezzo di storia. Esprimo pertanto un senso di affetto e di solidarietà - mi auguro di poter parlare anche a nome di tutto il Gruppo - nei confronti del sindaco della città di Pescara, Carlo Masci, che addirittura ha pianto dinanzi alle telecamere quando lo hanno intervistato, perché sentiva su

di sé la drammatica situazione del patrimonio forestale e storico di una città che andava in fumo, un fumo che addirittura ha lambito abitazioni civili, ha costretto anche molte suore ad abbandonare la propria sede per essere alloggiate presso un albergo della città.

Anch'io mi permetto di dire che in situazioni come queste bisogna sensibilizzare tutto il Parlamento affinché si adottino misure anche di prevenzione nei confronti di questo genere di necessità. Mi auguro che ovviamente in uno stato di emergenza come questo vi sia un occhio di riguardo verso una vicenda che non solo è diventata una notizia nei telegiornali di tutta Italia, ma che può essere un'occasione di vicinanza per gli amministratori locali della città di Pescara e dell'intera Regione Abruzzo. *(Applausi)*.

BAGNAI *(L-SP-PSd'Az)*. Domando di parlare.

PRESIDENTE. Ne ha facoltà.

BAGNAI *(L-SP-PSd'Az)*. Signor Presidente, desidero associarmi anch'io alle parole dei senatori D'Alfonso e Pagano per esprimere il mio sconcerto, che deve essere quello di tutti noi, di fronte a questa tragedia che ferisce la città di Pescara.

Sono luoghi - quelli che sono stati così ferocemente colpiti e devastati dalle fiamme - particolarmente cari a chi vi parla perché, fra l'altro, nell'immediata prossimità dell'università per tanti anni ho avuto l'onore di condurre la mia carriera: un polmone verde per la città, a ridosso delle abitazioni e degli stabilimenti balneari. È emersa ancora una volta con una tragica evidenza la fragilità di un territorio meraviglioso, ma esposto troppo spesso alla furia delle intemperie. Questo deve naturalmente suscitare in tutti noi una riflessione: in questo caso è stata la siccità, in altri casi sono state le bombe d'acqua, la grandine, a mettere in seria difficoltà la cittadinanza di Pescara e i suoi amministratori, cui va tutta la mia solidarietà, il mio affetto e la mia vicinanza in questo momento, nonché l'assicurazione - per quello che possiamo nel nostro ruolo di parlamentari del territorio - che tutto sarà fatto per cercare di rimediare agli esiti di questa terribile catastrofe.

Ringrazio lei, Presidente, e i colleghi che sono intervenuti per averci consentito di attirare l'attenzione su questo tremendo episodio. *(Applausi)*.

DI NICOLA *(M5S)*. Domando di parlare.

PRESIDENTE. Ne ha facoltà.

DI NICOLA *(M5S)*. Signor Presidente, il mio intervento arriva in coda a quello dei colleghi abruzzesi delle altre forze politiche che hanno già ricordato il dramma che in questo momento sta vivendo l'Abruzzo. E nel ricordare l'Abruzzo non possiamo dimenticare le altre zone del Paese colpite in questi giorni da incendi devastanti, a cominciare dalla Sardegna.

Non starò qui a ripetere le cose già dette sui danni, sui rischi che la stessa popolazione intorno a questi incendi e all'interno delle zone degli incendi ha corso e sta correndo.

Mi lasci dire una cosa, Presidente, per ricordare anzitutto a me stesso e a tutti che quando si parla di incendi spesso si dimentica di parlare di prevenzione.

È a tutti chiaro, per le notizie che stanno arrivando perlomeno dall'Abruzzo, che tali incendi sono frutto di mani dolose che appiccano sistematicamente il fuoco in zone in questo caso particolarmente care alla cultura abruzzese, ma negli anni scorsi anche all'interno di zone di montagna di gran pregio come il Gran Sasso. Si pensi anche all'incendio devastante - provocato anche in quel caso da mani dolose - intorno a Sulmona.

Voglio ricordare che in Abruzzo, nel mese di luglio, era arrivato l'allarme dei Vigili del fuoco che si lamentavano per il taglio dei fondi antincendio da parte della Regione.

Non voglio qui fare polemiche, ma quello che è successo ha dimostrato che l'allarme dei Vigili del fuoco era giustificato e se ne è vista la giustificazione proprio davanti alle dimensioni devastanti dei roghi.

Per questo ricordo a tutti noi che, piuttosto che continuare ogni anno a lamentare questi episodi, potremmo più concretamente cercare - anche all'interno del Senato - di avviare un'iniziativa, un'indagine conoscitiva per tentare di capire la dimensione del fenomeno e soprattutto tutti i mezzi che servono e che mancano a quella politica di prevenzione che tutto il Paese si aspetta. *(Applausi)*.

DE CARLO *(FdI)*. Domando di parlare.

PRESIDENTE. Ne ha facoltà.

DE CARLO *(FdI)*. Signor Presidente, pur non essendo abruzzese, sono legato particolarmente a quelle zone perché sono terre di alpini, come lo siamo noi bellunesi e veneti e, quindi, intervengo per portare la mia solidarietà alle genti e alle popolazioni che vivono oggi il dramma degli incendi.

Non è solo l'Abruzzo, che già basterebbe ad alzare un campanello d'allarme rispetto, da una parte, ai cambiamenti climatici e, dall'altra, alla stupidità umana di chi appicca fuoco in località così di pregio, come è accaduto a Pescara, ma anche in Sardegna, Sicilia e, come capita troppo spesso, in tante Regioni d'Italia.

È inutile parlare di prevenzione in un contesto parlamentare quando è stato il Parlamento nella legislatura scorsa a privarsi dell'unico Corpo che in Italia faceva prevenzione e, cioè, il Corpo forestale dello Stato. *(Applausi)*. Cerchiamo di far ritornare il discorso in un alveo un po' più di coerenza e, in qualche maniera, di onestà intellettuale. Quel Corpo non faceva solo repressione, che in tanti casi è dovuta, ma aveva anche - lo dico da sindaco - una grandissima funzione di prevenzione, di assistenza, di collaborazione e di coordinamento assieme alle forze e agli enti istituzionali come i Comuni, le Province e le Regioni. Smantellarlo, cambiarlo e dargli una destinazione diversa è stato un errore a cui possiamo porre rimedio. Ci sono un progetto di legge presentato alla Camera da Fratelli d'Italia, a mia prima firma, e un disegno di legge al Senato a prima firma della collega Rauti, che potrebbero recuperare la professionalità che esiste sul nostro territorio degli *ex* agenti del

Corpo forestale dello Stato proprio a tal fine. Oggi che non c'è più il Corpo forestale ci rendiamo conto di quanto sarebbe importante ed efficace in un'emergenza come quella che stiamo vivendo in Abruzzo.

Colleghi, basta parole di solidarietà e commenti vuoti; facciamo in modo di velocizzare l'*iter* di quei provvedimenti e ridiamo a questa Nazione il glorioso Corpo forestale dello Stato. *(Applausi)*.

DE PETRIS *(Misto-LeU-Eco)*. Domando di parlare.

PRESIDENTE. Ne ha facoltà.

DE PETRIS *(Misto-LeU-Eco)*. Signor Presidente, interveniamo non soltanto per esprimere la solidarietà alle popolazioni colpite, ma per sottolineare la gravità di quanto accaduto. Come ha detto il collega D'Alfonso, non solo sono andati in fumo 100.000 alberi, ma anche l'incomparabile valore storico e ambientale dell'ecosistema della pineta dannunziana.

Presidente, purtroppo in queste settimane non abbiamo fatto altro che assistere a incendi in Sardegna e in Sicilia. Quindi, vi è una situazione di grave emergenza. Lo dico anche al presidente D'Alfonso, che, magari, ci può essere d'aiuto per capire come intervenire.

Abbiamo davanti a noi un'emergenza con altissime temperature e con tutto ciò che ciò comporta e, come sempre, questi incendi sono di natura dolosa perché abbiamo trovato gli innesti. Allora mi chiedo cosa dobbiamo fare, perché questo serve.

Tra poco discuteremo della cybersicurezza, ma abbiamo un problema di sicurezza ambientale e di prevenzione. Abbiamo chiesto varie volte di poter utilizzare i droni e di fare un investimento della Protezione civile e dello Stato in modo da poter sorvegliare attentamente il territorio. Non dobbiamo dimenticare quello che sta accadendo adesso.

C'è un'altra questione. Lo dico sempre al collega D'Alfonso: è stato un errore grave aver sciolto il Corpo forestale dello Stato (l'inserimento all'interno dell'Arma dei carabinieri ne ha di fatto decretato lo smembramento) che svolgeva una grande funzione per quanto riguarda la prevenzione e il controllo - non è la stessa competenza affidata ai Vigili del fuoco - e che nei decenni conosceva benissimo il territorio.

Durante l'esame del decreto-legge reclutamento abbiamo presentato alcuni emendamenti che riguardano proprio il Corpo forestale, che ovviamente sono stati dichiarati improponibili, ma l'abbiamo fatto per sollevare la questione e chiedere - vedo il collega Toninelli, che ha fatto la stessa richiesta - che la Commissione affari costituzionali possa aprire un affare assegnato proprio sulla questione del Corpo forestale, sperando di riuscire a trovare delle soluzioni per porre rimedio a quello che è stato un errore gravissimo. Non dimentichiamolo, evitiamo di fare in modo che tra qualche settimana avremo dimenticato, perché quella della tutela del nostro territorio, dei nostri boschi e dei nostri ecosistemi è una vera e propria emergenza. *(Applausi)*.

PRESIDENTE. Vorrei unirmi anch'io alle parole di chi mi ha preceduto per esprimere la vicinanza, mia personale e penso di tutta l'Assemblea,

alle popolazioni che sono state colpite. Mi riferisco non soltanto agli incendi che hanno devastato l'Abruzzo, ma anche a quelli che hanno devastato la Sardegna e la Sicilia. Devo dire che è una tragedia che fa male davvero al cuore e ci fa pensare che non siamo soltanto in una situazione di emergenza: ogni volta si parla di emergenza, ma siamo in un'Italia fragile, quindi siamo in una situazione di pericolo costante. C'è stata di recente anche la questione di Como, che ha rivelato i problemi del dissesto idrogeologico. Siamo pertanto in presenza di un'Italia bella, ma molto, molto fragile. *(Applausi)*.

Sui lavori del Senato

PRESIDENTE. La Conferenza dei Capigruppo ha ridefinito il calendario della settimana corrente.

Nella seduta odierna si discuterà, fino alla sua conclusione, il decreto-legge in materia di cybersicurezza. A tal fine la seduta non prevede orario di chiusura.

L'ordine del giorno della seduta di domani, con inizio alle ore 11, prevede la discussione congiunta del rendiconto 2020 e dell'assestamento 2021, per le cui votazioni finali è richiesta la presenza del numero legale.

Saranno inoltre rese le comunicazioni del Presidente, ai sensi dell'articolo 126-*bis*, comma 2-*bis*, del Regolamento, sul disegno di legge di delega al Governo in materia di spettacolo, collegato alla manovra di finanza pubblica.

La seduta verrà quindi sospesa fino alle ore 16 e riprenderà con la discussione delle risoluzioni approvate dalle Commissioni riunite affari esteri e difesa sulla partecipazione dell'Italia a missioni internazionali. I tempi sono stati ripartiti tra i Gruppi per complessive tre ore, comprensive delle dichiarazioni di voto, fatti salvi i tempi dei relatori e del Governo.

Giovedì 5 agosto sarà discusso il decreto-legge sulla salvaguardia di Venezia e la tutela del lavoro.

Il *question time* già previsto per le ore 15 di giovedì non avrà luogo.

I lavori delle Commissioni riprenderanno dalla settimana del 30 agosto, ferma restando l'autorizzazione a convocarsi in qualunque momento, anche in data antecedente, in relazione a sopravvenute esigenze nelle materie di propria competenza.

L'Assemblea tornerà a riunirsi martedì 7 settembre, alle ore 16,30, con comunicazioni del Presidente sul calendario dei lavori, che sarà definito dalla Conferenza dei Capigruppo convocata nella stessa giornata di martedì 7 settembre, alle ore 15.

Ricordo che giovedì 5 agosto, alle ore 8,30, sarà convocata la Commissione monocamerale d'inchiesta sul gioco d'azzardo, per la propria costituzione.

Calendario dei lavori dell'Assemblea

PRESIDENTE. La Conferenza dei Presidenti dei Gruppi parlamentari, riunitasi oggi, con la presenza dei Vice Presidenti del Senato e con l'intervento del rappresentante del Governo, ha modificato - ai sensi dell'articolo 55 del Regolamento - il calendario della settimana corrente:

Martedì	3	agosto	h. 16,30	– Disegno di legge n. 2336 - Decreto-legge n. 82, Cybersicurezza *(approvato dalla Camera dei deputati) (scade il 13 agosto)* – Disegno di legge n. 2308 e 2309 - Rendiconto 2020 e Assestamento 2021 *(votazioni finali con la presenza del numero legale)* – Comunicazioni del Presidente, ai sensi dell'articolo 126-*bis*, comma 2-*bis*, del Regolamento, sul disegno di legge n. 2318 - Delega al Governo in materia di spettacolo *(collegato alla manovra di finanza pubblica)* – *Doc*. XXIV, n. 48, e *doc*. XXIV, n. 49 - Risoluzioni approvate dalle Commissioni riunite 3ª e 4ª sulla partecipazione dell'Italia a missioni internazionali **(mercoledì 4, ore 16)** – Disegno di legge n. 2329 - Decreto-legge n. 103, Salvaguardia di Venezia e tutela del lavoro *(voto finale entro il 20 agosto) (scade il 18 settembre)* **(giovedì 5)**
Mercoledì	4	"	h. 11-20	
Giovedì	5	"	h. 9,30-20	

I lavori delle Commissioni riprenderanno dalla settimana del 30 agosto, ferma restando l'autorizzazione a convocarsi in qualunque momento, anche in data antecedente, in relazione a sopravvenute esigenze nelle materie di propria competenza.

Martedì	7	settembre	h. 16,30	– Comunicazioni del Presidente sul calendario dei lavori

Ripartizione dei tempi per la discussione del disegno di legge n. 2336 (Decreto-legge n. 82, Cybersicurezza)

(5 ore, escluse dichiarazioni di voto)

Relatori		20'

Governo		20'
Votazioni		20'
Gruppi 4 ore, di cui:		
M5S		43'
L-SP-PSd'Az		39'
FIBP-UDC		34'
Misto		33'+5'
PD		29'
FdI		23'+5'
IV-PSI		21'
Aut (SVP-PATT, UV)		18'
Dissenzienti		da stabilire

Ripartizione dei tempi per la discussione dei disegni di legge nn. 2308 e 2309
(Rendiconto 2020 e Assestamento 2021)
(4 ore, escluse dichiarazioni di voto)

Relatori		20'
Governo		20'
Votazioni		20'
Gruppi 4 ore, di cui:		
M5S		32'
L-SP-PSd'Az		29'
FIBP-UDC		25'
Misto		25'+5'
PD		22'
FdI		17'+5'

IV-PSI		16'
Aut (SVP-PATT, UV)		14'
Dissenzienti		da stabilire

Ripartizione dei tempi per la discussione dei *doc*. XXIV, n. 48, e XXIV, n. 49
(Risoluzioni approvate dalle Commissioni riunite 3ª e 4ª sulla partecipazione dell'Italia a missioni internazionali)
(3 ore, escluse dichiarazioni di voto)

M5S		32'
L-SP-PSd'Az		29'
FIBP-UDC		25'
Misto		25'
PD		22'
FdI		17'
IV-PSI		16'
Aut (SVP-PATT, UV)		13'
Dissenzienti		da stabilire

Ripartizione dei tempi per la discussione del disegno di legge n. 2329
(Decreto-legge n. 103, Salvaguardia di Venezia e tutela del lavoro)
(5 ore, escluse dichiarazioni di voto)

Relatori		20'
Governo		20'
Votazioni		20'
Gruppi 4 ore, di cui:		
M5S		43'
L-SP-PSd'Az		39'

FIBP-UDC		34'
Misto		33'+5'
PD		29'
FdI		23'+5'
IV-PSI		21'
Aut (SVP-PATT, UV)		18'
Dissenzienti		da stabilire

Discussione e approvazione del disegno di legge:
(2336) ***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*** *(Approvato dalla Camera dei deputati) (Relazione orale)* **(ore 17,06)**

PRESIDENTE. L'ordine del giorno reca la discussione del disegno di legge n. 2336, già approvato dalla Camera dei deputati.

La relatrice, senatrice Mantovani, ha chiesto l'autorizzazione a svolgere la relazione orale. Non facendosi osservazioni la richiesta si intende accolta.

Pertanto, ha facoltà di parlare la relatrice.

MANTOVANI, *relatrice*. Signor Presidente, il provvedimento in esame reca la conversione in legge del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in tema di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale. Ricordo preliminarmente che la sicurezza cibernetica costituisce uno degli interventi previsti dal Piano nazionale di ripresa e resilienza e rappresenta uno dei sette investimenti della digitalizzazione della pubblica amministrazione, primo asse di intervento della componente 1 "Digitalizzazione, innovazione e sicurezza nella pubblica amministrazione", compresa nella missione 1 "Digitalizzazione, innovazione competitività, cultura e turismo".

Il testo del decreto-legge, già approvato con modificazioni dalla Camera dei deputati, si compone di 19 articoli. Gli articoli da 1 a 4 definiscono il sistema nazionale di sicurezza cibernetica, che ha al suo vertice il Presidente del Consiglio dei ministri. Nello specifico, l'articolo 1 reca alcune definizioni utilizzate nel decreto-legge. L'articolo 2 attribuisce in via esclusiva al Presidente del Consiglio dei ministri l'alta direzione e la responsabilità generale delle politiche di cybersicurezza, l'adozione della relativa strategia nazionale,

nonché la nomina e la revoca del direttore generale e del vice direttore generale della nuova Agenzia per la cybersicurezza nazionale, istituita dall'articolo 5. Di tali nomine sono preventivamente informati il Comitato parlamentare per la sicurezza della Repubblica (Copasir) e le Commissioni parlamentari competenti.

L'articolo 3 prevede che il Presidente del Consiglio dei ministri possa delegare all'Autorità delegata per il sistema di informazione per la sicurezza della Repubblica, ove istituita, le funzioni che non sono attribuite a lui in via esclusiva. L'Autorità delegata è tenuta a informare costantemente il Presidente del Consiglio, il quale, fermo restando il potere di direttiva, può in qualsiasi momento avocare a sé l'esercizio di tutte o di alcune funzioni. L'Autorità delegata, in relazione alle funzioni esercitate, ai sensi del presente decreto-legge, partecipa alle riunioni del Comitato interministeriale per la transizione digitale, di cui all'articolo 8 del decreto-legge n. 22 del 2021.

L'articolo 4 istituisce presso la Presidenza del Consiglio dei ministri il Comitato interministeriale per la cybersicurezza (CIC), organismo con funzioni di consulenza, proposta e vigilanza. Al Comitato sono attribuiti i seguenti compiti: proporre al Presidente del Consiglio gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale; esercitare l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza; promuovere l'adozione di iniziative per favorire la collaborazione a livello nazionale e internazionale tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza; esprimere il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la cybersicurezza nazionale. Il Comitato è presieduto dal Presidente del Consiglio ed è composto dall'autorità delegata e dai Ministri degli affari esteri e della cooperazione internazionale, dell'interno, della giustizia, della difesa, dell'economia e delle finanze, dello sviluppo economico, della transizione ecologica, dell'università e della ricerca, delle infrastrutture e della mobilità sostenibili e dal Ministro delegato per l'innovazione tecnologica. Le funzioni di segretario del Comitato sono svolte dal direttore generale dell'Agenzia per la cybersicurezza nazionale. Possono partecipare alle sedute del Comitato, senza diritto di voto, altri componenti del Consiglio dei ministri e altre autorità civili e militari, di cui di volta in volta si ritenga necessaria la presenza in relazione alle questioni da trattare. Infine, sono trasferite al CIC le funzioni già attribuite al Comitato interministeriale per la sicurezza della Repubblica (CISR) dal decreto-legge n. 105 del 2019 (cosiddetto decreto-legge perimetro) e dai relativi provvedimenti attuativi, fatta eccezione per quelle previste all'articolo 5 del medesimo decreto-legge in tema di disattivazione di apparati o prodotti in caso di rischio grave e imminente per la sicurezza nazionale, connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici.

Seguono una serie di disposizioni che riguardano l'Agenzia per la cybersicurezza nazionale, organo strumentale all'esercizio delle competenze che il decreto-legge assegna al Presidente del Consiglio e all'autorità delegata.

L'articolo 5 ne prevede l'istituzione, dotandola di personalità giuridica di diritto pubblico e di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, nei limiti di quanto previsto dal decreto in esame. In particolare, il decreto-legge prevede l'adozione dei seguenti regolamenti: regolamento di organizzazione e funzionamento; regolamento di contabilità; regolamento sulle procedure per la stipula di contratti di appalti, di lavori e di forniture per le attività finalizzate alla sicurezza; regolamento del personale. L'articolo 6 disciplina l'organizzazione dell'Agenzia, al cui vertice figura il direttore generale, che è il legale rappresentante dell'Agenzia, nonché il diretto referente del Presidente del Consiglio e dell'autorità delegata. L'articolo 7 definisce le numerose funzioni dell'Agenzia, riconosciuta come autorità nazionale per la cybersicurezza, come autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, nonché come autorità nazionale di certificazione della cybersicurezza.

Ulteriori disposizioni riferite all'Agenzia si rinvengono nell'articolo 11, relativo a risorse finanziarie e autonomia contabile; nell'articolo 12, che disciplina il personale, e nell'articolo 14, con riferimento alle relazioni annuali che il Presidente del Consiglio è tenuto a trasmettere al Parlamento e al Copasir sull'attività dell'Agenzia.

Gli articoli 8 e 9 riguardano la costituzione, presso l'Agenzia, di un nucleo per la cybersicurezza per gli aspetti relativi alla prevenzione e alla preparazione a eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento. L'articolo 10 riguarda la gestione delle crisi che coinvolgano aspetti della cybersicurezza. L'articolo 13 ha per oggetto la trattazione dei dati personali per finalità di sicurezza nazionale e cibernetica. L'articolo 15 detta una serie di novelle al decreto legislativo n. 65 del 2018, che ha dato attuazione alla direttiva UE 2016/1148, cosiddetta direttiva Network and Information Security (NIS), al fine di armonizzarlo con l'impianto normativo proprio del decreto-legge in esame. L'articolo 16 novella al medesimo scopo altri atti normativi. L'articolo 17 reca disposizioni transitorie e finali, mentre l'articolo 18 contiene disposizioni finanziarie. L'articolo 19 dispone in merito all'entrata in vigore. *(Applausi)*.

PRESIDENTE. Dichiaro aperta la discussione generale.

È iscritta a parlare la senatrice Binetti. Ne ha facoltà.

BINETTI *(FIBP-UDC)*. Signor Presidente, membri del Governo, colleghi, l'asciutta relazione che abbiamo appena ascoltato nelle parole della relatrice dà sicuramente un'idea dell'architettura di un sistema, ma forse non riesce a darci fino in fondo la dimensione profonda che i problemi di *cybersecurity* hanno sotto una serie di aspetti che ci toccano molto da vicino. Nel caso concreto mi piace soffermarmi sull'impatto che tali aspetti hanno in tema di salute.

Voi sapete - è parte integrante del Piano nazionale di ripresa e resilienza - che la transizione digitale rappresenta il presupposto per consentire alle organizzazioni che compongono il Sistema sanitario nazionale di rag-

giungere gli obiettivi che sono stati messi a fuoco proprio nella grande operazione di modernizzazione del nostro Paese, che parte appunto dal nostro Sistema sanitario, dandogli nuova linfa dall'interno e modificandone la dimensione, finora fortemente ospedalocentrica, per aprirla ad abbracciare le infinite misure che possono riguardare una sanità più attiva sui territori. La transizione digitale assume perciò una rilevanza strategica e trasversale rispetto a tutti gli altri temi trattati.

Per tale motivo occorre semplificare l'accesso ai servizi sanitari e socio-assistenziali, anche ridisegnando un modello di Sistema sanitario nazionale che sappia accompagnare il paziente fin dall'inizio della fruizione dei servizi, includendo la continuità ospedale-territorio, l'integrazione, la collaborazione sociosanitaria, lo sviluppo dell'assistenza domiciliare, grazie alla definizione di adeguati percorsi diagnostico-terapeutici. Ma nulla di tutto ciò potrebbe essere fatto senza una forte, chiara, esplicita e - mi si passi il termine - rivoluzionaria transizione tecnologica, che consegni al sistema digitale la gestione di dati di una delicatezza infinita, come sono tutti i dati che riguardano la nostra salute e, in un certo senso, la nostra identità personale. È la grande rivoluzione che la tecnologia farà attraverso la transizione digitale, di cui - attenzione - si assume in prima persona la responsabilità il Presidente del Consiglio. Il tema della *cybersecurity* ha nel Presidente del Consiglio il suo punto di riferimento e noi ci auguriamo che - costi quello che costi - la transizione si faccia a garanzia della salute, a garanzia dei dati e della *privacy* di ognuno di noi, a garanzia dell'efficacia e dell'efficienza.

Proprio per questo nella 12ª Commissione, discutendo oggi su questo provvedimento, abbiamo espresso un parere ovviamente favorevole, ma con un'osservazione, che mi piace richiamare all'attenzione di tutta l'Assemblea: nella cabina di regia, tra le tante autorevoli persone chiamate a farne parte, ci sia anche il Ministero della salute. È infatti in gioco certamente la salute del sistema, ma anche la salute di ognuno di noi. Per questo è necessario che, quando si parla di *cybersecurity* e di investimenti massicci, che vengono fatti non solo sul digitale in senso generico, ma in particolare sulla sanità digitale, in quel cervello organizzativo siano presenti persone esperte di sanità.

Credo che questo possa essere un momento molto positivo per modificare in meglio il Sistema sanitario nazionale e generare quei piani nazionali che finora erano destinati ad essere parcheggiati in un cassetto, che sia il Piano sanitario nazionale sotto il profilo oncologico, quello sulle malattie rare o quello sulla cronicità. Tutto questo può essere rivitalizzato se le reti informatiche saranno capaci di intercettare i bisogni reali e di offrire ad essi risposte.

Credo, quindi, che sia un momento molto positivo per combinare la tecnologia con quelle che chiamiamo le *medical humanities*, e cioè quell'umanizzazione della medicina... *(Il microfono si disattiva automaticamente). (Applausi)*.

PRESIDENTE. È iscritta a parlare la senatrice Minuto. Ne ha facoltà.

MINUTO *(FIBP-UDC)*. Signor Presidente, il recentissimo attacco *hacker* al sistema informatico della Regione Lazio ci ha fatto comprendere, qualora ce ne fosse ancora bisogno, che la minaccia cibernetica è in realtà

concreta e prossima alla vita dei cittadini comuni. I *malware*, sempre più sofisticati, non solo offendono gli interessi strategici del Paese, ma possono anche colpire direttamente le persone, sottraendo loro risorse economiche, accesso alle fonti energetiche, ai trasporti e alle cure.

Nel caso di questo attacco si sarebbe trattato di un *ramsonware* con finalità estorsive, che ha creato un ritardo nel funzionamento del sistema regionale di vaccinazione, che opera nell'ambito dell'efficiente coordinamento nazionale affidato alla professionalità del grande generale Figliuolo, e potrebbe essere stato la causa di altre infezioni che si sarebbero potute naturalmente evitare. Lo stesso tipo di attacco ha recentemente paralizzato il sistema sanitario irlandese e il grande oleodotto americano. Anche durante le guerre, le istituzioni sanitarie del nemico sono protette da convenzioni internazionali; gli attacchi informatici, invece, non hanno regole e i loro scopi spesso non sono facilmente decifrabili, come l'identità dei loro autori.

Non possiamo dunque che giudicare opportuna e necessaria l'istituzione dell'Agenzia per la cybersicurezza nazionale, che colma un vuoto ormai anacronistico tra gli strumenti per la difesa degli interessi e degli *asset* nazionali. La delicata fase della transizione digitale della pubblica amministrazione deve essere protetta e guidata dagli esperti dell'Agenzia, anche per evitare che si perpetui l'assurda situazione che i sistemi informatici delle istituzioni siano notevolmente più fragili e arretrati rispetto ai sistemi detenuti dai privati. I sistemi informatici delle pubbliche amministrazioni contengono i dati più riservati dei cittadini e dovrebbero essere difesi dalle incursioni criminali, con la stessa cura riservata ai servizi segreti vitali dello Stato. La sicurezza dei dati dei cittadini diventerà ancor più cogente dal momento che verrà creato il fascicolo sanitario elettronico omogeneo a livello nazionale, che diventerà il singolo punto di accesso, per cittadini e residenti, alla propria storia clinica e ai servizi offerti dal Servizio sanitario nazionale.

Altro aspetto della trasformazione digitale della pubblica amministrazione, prescritta dal PNRR, sarà la migrazione delle amministrazioni sul *cloud* e l'interoperabilità dei sistemi informatici, accentramento telematico che dovrà avvenire in un ambiente rigorosamente presidiato.

Auspico che l'Agenzia possa essere una struttura agile e reattiva e non posso che apprezzare il fatto che essa risponderà direttamente al Presidente del Consiglio dei ministri e all'Autorità delegata per la sicurezza della Repubblica, nel pieno rispetto delle prerogative del Parlamento. Ma il rafforzamento della cybersicurezza del comparto pubblico potrebbe essere inefficiente se non si provvederà a una robusta campagna di informazioni al largo pubblico sui temi della sicurezza informatica.

Colleghi, noi tutti sappiamo che anche un solo *personal computer* infettato può essere la base di partenza di attacchi informatici devastanti. L'educazione alla sicurezza informatica dovrebbe essere materia di insegnamento, come lo è la sicurezza stradale.

L'Agenzia sarà il centro nazionale di coordinamento che si rapporterà con gli omologhi organismi internazionali, un presidio importante per la protezione dei nostri cittadini che avvicinerà l'Italia ai più alti *standard* di sicurezza. *(Applausi)*.

PRESIDENTE. È iscritta a parlare la senatrice Tiraboschi. Ne ha facoltà.

TIRABOSCHI *(FIBP-UDC)*. Signor Presidente, colleghi, rappresentanti del Governo, come ha detto bene il relatore, la *cybersecurity* è il pilastro fondamentale dell'economia digitale ed è per questo che dobbiamo intendere l'Agenzia che si vuole istituire come un'organizzazione al servizio della *governance.*

Se non facciamo questo salto, si tratterà dell'ennesima sovrastruttura, peraltro - questi temi vengono affrontati già da quattro, cinque anni - regolamentata già in precedenza, e di cui noi abbiamo chiaramente ridefinito il perimetro, le attività, le finalità e gli obiettivi. Sono accadute una serie di cose - pensiamo all'attacco alla Regione Lazio - che ci devono assolutamente far riflettere.

Il provvedimento sulla *cybersecurity* è quindi un'ottima iniziativa, a condizione che non si pensi che l'organizzazione possa far fronte da sola agli attacchi e soprattutto a quelli definiti *nation-state*. La sicurezza è un ecosistema che si costruisce facendo squadra con i maggiori *player* internazionali e definendo le *partnership* tra pubblico e privato.

A tal proposito, apro una parentesi. Una serie di gare d'appalto è stata aggiudicata a fornitori privati e nei capitolati non si è prestata alcuna attenzione ai temi della *cybersicurezza.* Tenete presente che una parte significativa di manutenzione applicativa e ai sistemi viene fatta proprio da aziende private e si costruisce lasciando al privato tutte le attività di *threat intelligence* e *threat analysis* e riservando invece al pubblico le attività di *intelligence* sulle questioni più sociologiche, psicologiche, comportamentali, culturali e politiche.

A tal riguardo, sarebbe auspicabile una forte cooperazione internazionale tra le Agenzie di *intelligence* perché è fondamentale conoscere il nemico. Il nemico del terzo millennio non è colui che lancia aerei e carri armati come fossero delle bombe, ma è un vero e proprio pirata, un soggetto che non ha Patria, né scrupoli e che, con un *click* su un *computer,* che si trova magari dall'altra parte del mondo, può scatenare vere e proprie guerre; guerre che si scatenano oggi bloccando gli aeroporti, gli ospedali, la comunicazione e tutto ciò che vive e funziona attraverso le connessioni. *(Applausi)*. Pensate addirittura che oggi delle mani esperte potrebbero bloccare un'auto di ultima generazione con il passeggero che si trova all'interno. Insomma, si tratta di temi assolutamente da non sottovalutare.

Come sappiamo perfettamente, le nuove guerre si combattono nel cyberspazio e noi stiamo cedendo in maniera del tutto gratuita - e, se vogliamo, anche inconsapevole - tutto quello che possediamo. E ciò avviene perché non abbiamo mai investito sulla formazione generalizzata e diffusa che pervade l'economia reale e che - secondo me - dovrebbe iniziare fin dalla scuola materna. I ragazzini "smanettano" sui *device* e, quindi, non sarebbe male pensare a introdurre il digitale come materia scolastica, in quanto la cultura deve crescere dal basso.

Che cosa si può fare? Penso a un'infrastruttura di sicurezza nazionale intesa come una porta o finestra blindata - e non basterebbe comunque solo

questa - e anche a delle piattaforme. I tecnici utilizzano il termine di *security operations center* (SOC) per indicare quegli strumenti che sono fondamentali soprattutto se messi a disposizione della piccola e media impresa, che non ha le competenze, né le risorse per poter far fronte a degli attacchi. Sapete quanta gente si accorge del furto di un *computer*, ma non di quello di dati?

Come ho detto, serve una formazione che sia capillare... *(Il microfono si disattiva automaticamente).*

PRESIDENTE. È iscritto a parlare il senatore Aimi. Ne ha facoltà.

AIMI *(FIBP-UDC)*. Signor Presidente, signor rappresentante del Governo, colleghi, siamo sicuramente al centro di una grande rivoluzione tecnologica - lo vediamo quotidianamente - e la sicurezza dei nostri sistemi informatici assume una centralità assoluta.

Nulla è più come prima. Come ricordava la collega Tiraboschi, siamo abituati a conflitti internazionali di stampo bellico, con l'utilizzo magari di carri armati, di razzi, di aerei, ma oggi siamo di fronte a uno scenario completamente diverso, che ci deve far riflettere e che vede l'Italia in una condizione di assoluta fragilità e vulnerabilità.

Dobbiamo reagire e credo che la risposta che stiamo dando quest'oggi sia adeguata, ma dobbiamo sicuramente fare di più. Dobbiamo imparare a proteggere i nostri confini, innanzitutto quelli geografici, quelli terrestri e marittimi, che meritano pur sempre una grande attenzione, perché non esiste una Nazione senza confini. Vanno però protetti anche i confini del cyberspazio, i confini della tecnologia, quelli che attengono alle grandi strutture e infrastrutture. Penso - ad esempio - all'attacco alla Regione Lazio al quale si è fatto riferimento, con l'utilizzo di *hacker* che sono riusciti a sfondare le linee, mettendo in grave difficoltà la campagna vaccinale della Regione e lo stesso sistema del *green pass*, determinando una situazione che non ci saremmo aspettati prima.

La difesa del cyberspazio diventa quindi fondamentale, perché proteggiamo sicuramente noi stessi, i nostri affetti, la nostra casa, ma dobbiamo proteggere l'Italia e, con essa, l'Europa, che si è già attivata a partire dal 2016 per richiedere maggiore attenzione su questo tema così delicato.

Si tratta dunque di una questione di assoluta sovranità, che passa, circola e viaggia senz'altro di fianco a noi e sopra di noi.

Abbiamo quindi la necessità di dare un monito, soprattutto alla politica, facendo attenzione anche alla classe dirigente che sarà chiamata a guidare il Paese: già sono stati 300 gli assunti, ma abbiamo necessità di avere personale altamente qualificato.

Durante la Seconda guerra mondiale - correva l'anno 1941 - il Regno Unito, entrato in guerra da ormai due anni, si trovò di fronte a una situazione gravissima: se è vero che aveva radar e mezzi bellici molto importanti, è altrettanto vero che non riusciva a decodificare il codice enigma che veniva utilizzato dall'Asse. Per fare questo venne pubblicato sostanzialmente un enigma di difficilissima soluzione sul «The Daily Telegraph», un cruciverba particolare. Risposero in tantissimi, ma solo pochi riuscirono a dare la risposta

giusta. Ebbene, i Servizi segreti di sua Maestà intervennero, riuscendo ad arruolare quelle persone in una grande operazione di crittoanalisi così da decodificare il codice enigma. A farlo furono linguisti, giocatori di scacchi, matematici, scienziati, persone di altissimo livello.

Noi abbiamo la necessità di ricercare chi ha queste grandi capacità; in particolare, dovremmo anche testare la loro straordinaria fedeltà perché - come comprendete bene - su temi così delicati si deve andare in questa direzione.

La sicurezza nazionale riguarda dunque non solamente l'economia, ma anche le strutture militari.

Il 29 luglio abbiamo avuto un attacco. Dobbiamo rispondere con forza; non basta probabilmente il codice penale, con l'articolo 615-*ter* e, soprattutto, con la previsione del reato di tentata estorsione. Noi dobbiamo intervenire pesantemente.

Credo che Forza Italia abbia partecipato in maniera fondamentale nel dare un contributo significativo al miglioramento del provvedimento in esame. *(Applausi)*.

PRESIDENTE. È iscritto a parlare il senatore Grimani. Ne ha facoltà.

GRIMANI *(IV-PSI)*. Signor Presidente, onorevoli colleghi, onorevole rappresentante del Governo, siamo chiamati oggi a votare per il disegno di legge di conversione del decreto-legge in materia di cybersicurezza, un tema importante nell'ottica della progettazione del futuro, una delle sfide più grandi e più complesse che dovranno affrontare tutte le società del mondo.

Due sono i punti di partenza da analizzare: il primo riguarda il rischio e sostanzialmente la vulnerabilità a cui è esposto il sistema informatico; il secondo riguarda il fatto che il dominio digitale sarà sempre uno dei fattori più determinanti per la concorrenza tra gli Stati. Il tema degli attacchi informatici ha caratterizzato gli ultimi anni in tutto il mondo; attacchi stranieri che hanno riguardato - ad esempio - i nostri Comuni, per non parlare della Colonial Pipeline, un oleodotto statunitense. Il sistema industriale mondiale molto spesso ha visto i propri sistemi hackerati, come nel caso delle acciaierie o del colosso della navigazione Maersk. Sono stati tanti gli esempi che si sono succeduti nel mondo negli ultimi anni, per non parlare della vicenda che ha riguardato la Regione Lazio recentemente.

Gli attacchi informatici determinano dei costi per il sistema, costi legali, costi normativi e costi informatici, e c'è bisogno di dare delle risposte per ridurre tali costi e i rischi per i nostri cittadini. Per questo è stato fondamentale far crescere una radicata cultura della cybersicurezza, perché sono esposti ai rischi le pubbliche amministrazioni da un lato, ma anche il tessuto economico privato dall'altro. Spesso, il tessuto economico, soprattutto quello delle piccole e medie imprese, è molto esposto, perché i sistemi di sicurezza delle stesse sono deboli e le imprese non hanno le risorse sufficienti per far fronte ai costi.

Se facciamo un paragone con il resto d'Europa, si impone una riflessione per evidenziare perché fosse così necessario un intervento nel nostro Paese. La Germania ha un'agenzia sulla cybersicurezza nata già nel 1991 con

1.200 dipendenti. Anche in Francia esiste un'agenzia che ha oltre mille dipendenti. Noi abbiamo preso consapevolezza di questo tema della cybersicurezza nel 2017, quando lo abbiamo reinserito nel comparto dell'*intelligence*. Dobbiamo valutare - e il Governo lo ha fatto - che è un problema non solo di *intelligence*, ma è molto più complesso e riguarda altri ambiti, soprattutto la cooperazione pubblico-privato, come ho detto prima.

Ben venga, quindi, il disegno di legge al nostro esame che Italia Viva ha sostenuto con convinzione anche alla Camera, che prevede un vertice snello, la Presidenza del Consiglio, come riferimento fondamentale della nuova Agenzia. Ci sono stati un rafforzamento delle Commissioni, un rafforzamento del ruolo del Copasir e un'azione di monitoraggio del Parlamento che dovrà essere svolta anche in futuro per quanto riguarda le iniziative che deve mettere in campo la nuova Agenzia.

Il tema della cybersicurezza, quindi, è complesso ma va affrontato, soprattutto perché la nostra pubblica amministrazione ha un *server* piuttosto esposto da questo punto di vista. Ben venga quindi questo tipo di iniziativa. L'obiettivo dovrà essere una connettività sempre maggiore e diffusa ovunque, che è il carattere fondamentale delle società moderne. Dobbiamo guardare avanti: la rete e l'informatizzazione aprono nuove prospettive di crescita sul piano occupazionale e su quello dei servizi. Dobbiamo proteggere le reti e l'informatizzazione. Non dobbiamo girarci dall'altra parte, ma anzi dobbiamo sostenere con convinzione il progresso.

Noi riformisti accettiamo questa sfida, non ci chiudiamo a riccio, non abbiamo lo sguardo rivolto al passato, ma anzi guardiamo al futuro e crediamo che la società vada cambiata e resa più sicura. In questo senso, l'impegno che il Governo ha manifestato con il provvedimento in esame viene fortemente sostenuto dal Parlamento in maniera trasversale agli schieramenti di partenza di maggioranza e opposizione. È un impegno che sosteniamo con convinzione perché riguarda il futuro e la sicurezza del Paese. Sarà importante lavorare in questo ambito garantendo un impegno continuo del Parlamento, che sarà fondamentale per quanto riguarda l'analisi dello stato di avanzamento dell'Agenzia e del suo funzionamento, che è l'aspetto cruciale del decreto-legge in conversione che ci apprestiamo ad approvare. *(Applausi)*.

PRESIDENTE. È iscritto a parlare il senatore Malan. Ne ha facoltà.

MALAN *(FdI)*. Signor Presidente, la questione della cybersicurezza e della sicurezza informatica è estremamente importante. Sempre più affidiamo i nostri dati di ogni tipo alla Rete, a supporti informatici; indubbiamente ciò velocizza una serie di processi e consente di realizzare una serie di comodità e di economie estremamente importanti, come lo è essere aggiornati in questo settore.

Tuttavia, il fatto che questo strumento sia ormai fondamentale per la gestione di quasi qualunque settore delle nostre attività ci espone a particolari pericoli e ciò vale per tantissimi ambiti, dalla sicurezza militare, alla sicurezza governativa, a quella delle strutture del Governo, dei dati sanitari, dei dati

bancari. È una serie enorme, difficile da completare, perché oramai tutti i nostri settori si affidano a questo supporto, a questa tecnologia. La sicurezza in questo campo è dunque fondamentale, come è già stato detto.

Altri Paesi sono molto più avanti di noi, hanno delle strutture che già lavorano da anni, con grande grande supporto di mezzi e di personale. Noi siamo indietro. Il Governo precedente ha fatto il possibile per farci rimanere indietro con degli stravaganti progetti di affidare la gestione della sicurezza informatica a società private; tali progetti avevano il grosso difetto non soltanto di essere insensati in sé, ma anche di aver fatto perdere molto tempo. Adesso, con il provvedimento in esame finalmente si prende atto di una realtà importante.

Si tratta di una questione ad altissima competizione, perché nelle università più serie e accreditate, dove l'ingegneria informatica è ai massimi livelli, le esercitazioni principali per quanto riguarda la sicurezza, che - come sappiamo benissimo - è fondamentale, vengono fatte nel modo seguente: metà degli studenti lavora come se fosse una banca, un Ministero, un'azienda, una qualunque entità che abbia interesse a tutelare i propri dati e a non far entrare estranei; un'altra metà degli studenti fa il lavoro opposto, quello dello *hacker,* del pirata cibernetico. Dico questo per chiarire che ci vogliono personale, una tecnologia, una strutturazione ai massimi livelli, perché in questo ambito il secondo posto non serve: al primo posto c'è la società, l'entità, il Ministero, il reparto militare che riesce a mantenere la propria sicurezza, mentre al secondo c'è il soggetto che non riesce e cioè perde.

Bisogna quindi attrezzarsi, pensare di avere ambizioni che vanno molto oltre rispetto a quanto previsto dal decreto-legge in esame che pure - come ho detto -rappresenta un passo nella direzione giusta dal punto di vista sia della quantità, per cui bisogna dotarsi delle strutture, delle risorse umane, tecnologiche e finanziarie necessarie, sia della qualità.

Mi è caduto l'occhio sull'articolo 8 del provvedimento concernente il nucleo per la cybersicurezza, che dovrebbe essere proprio la punta di diamante dove si mettono a punto le strategie più avanzate, dove ci devono essere le idee migliori. Sappiamo bene cosa è stato inserito per far quadrare i conti, perché non ci siano questioni di copertura. È stato inserito questo comma, nel quale si dice che ai componenti del nucleo non spettano compensi, gettoni di presenza e rimborsi spese o altri emolumenti comunque denominati. Questa è una bellissima, virtuosa, direi pauperistica affermazione, ma ho qualche dubbio che sia possibile attirare le competenze necessarie a queste condizioni: zero soldi, zero compensi, zero rimborsi spese. Magari qualcuno ci andrà pure, ma noi abbiamo bisogno dei migliori, bisogna prendere molto sul serio quanto tutti stiamo dicendo, vale a dire che sulla rete si combattono le guerre. Già accade oggi ed è accaduto in passato, non è qualcosa di futuribile, che potrà accadere tra cinque, dieci o vent'anni. Dobbiamo quindi attrezzarci - anzi dovevamo farlo ancora prima - e dobbiamo essere coscienti che bisogna avere le armi migliori, perché l'arco contro la mitragliatrice non ce la fa, anche se è un'arma rispettabile. Bisogna essere attrezzati, bisogna avere un approccio assolutamente strutturale, perché qui non c'è differenza tra militare e non militare, tra un settore e l'altro, fra l'interno e l'estero: la rete è globale, la

minaccia dunque è globale, può arrivare da qualunque parte del pianeta, naturalmente può anche arrivare dall'interno del nostro Paese e la vittima può essere chiunque. Non c'è neanche una distinzione dal punto di vista della vulnerabilità e della strategicità delle possibili conseguenze di un attacco che subiamo e che tale attacco abbia successo, perché non c'è differenza tra pubblica amministrazione e privati, perché non c'è differenza tra colpire una grande azienda, una banca, oppure una struttura dello Stato. Le conseguenze rischiano per tutti di essere molto gravi. C'è quindi un grande lavoro da fare, ma in questo provvedimento c'è un inizio che francamente riteniamo ancora ben lontano dall'essere sufficiente e abbiamo anche, in alcuni aspetti relativi al modo in cui vengono strutturati questi ordini del giorno, una certa consapevolezza che tutto deve essere in capo al Governo mentre l'opposizione, che oggi è costituita da Fratelli d'Italia e domani sarà costituita da altri, viene un po' tenuta da parte. Questo è un tema di interesse nazionale, che interessa tutti, non si può escludere nessuno, non si possono includere nel comitato ministeriale alcuni Ministeri, magari perché oggi sono occupati da esponenti di certe forze politiche o di certe correnti culturali, e tenerne fuori altri perché non fanno parte invece di quei settori.

C'è un gran lavoro da fare, questo è un primo passo ma la questione della cybersicurezza deve essere trattata con grande serietà e con la coscienza che ci coinvolge tutti, che c'è bisogno della collaborazione di tutti, delle menti e delle idee migliori. Abbiamo presentato i nostri emendamenti e ordini del giorno per dare un contributo, bisogna andare avanti e molto su questa strada. *(Applausi)*.

PRESIDENTE. È iscritto a parlare il senatore Mallegni. Ne ha facoltà.

MALLEGNI *(FIBP-UDC)*. Signor Presidente, che ci volesse un'Agenzia per la cybersicurezza l'avevamo detto più volte; anzi, qualcuno ci aveva anche già provato nella scorsa legislatura, poi la questione era stata stoppata. In seguito si è ripreso un cammino rispetto a questo tema e proprio in questi giorni - nella vita serve anche la fatalità - la Regione Lazio subisce l'attacco informatico e il Parlamento si trova ad approvare il disegno di legge perché questa Agenzia per la cybersicurezza possa nascere.

La sicurezza è fondamentale, come lo sono la *privacy* e la libertà: non dimentichiamolo mai, neppure quando andiamo a scrivere e poi a votare, come stiamo facendo oggi, un provvedimento sulla cybersicurezza.

Mi piacerebbe sapere in quanti hanno letto il testo; sarei curiosissimo di sapere nel dettaglio quanti colleghi hanno letto tutti gli articoli del decreto-legge sulla cybersicurezza. Lo dico perché francamente, seppur siamo totalmente d'accordo sull'istituzione dell'Agenzia, vorrei chiedere a tutti se sanno che, a metà articolato, tale Agenzia diventa l'Autorità nazionale per la cybersicurezza. Mi piacerebbe sapere se tutti hanno letto che gli stipendi delle 300 persone che vi lavoreranno sono adeguati alla Banca d'Italia, soggetto di diritto privato, quindi non legato ai tetti. Poi non vi lamentate se gli stipendi sono alti! D'altra parte, è anche giusto che sia così, ci mancherebbe altro. Tuttavia, nella vita serve coraggio: se vogliamo fare questa scelta attiviamo lo *spoil system*, assumiamoci la responsabilità, andiamo a scegliere i migliori. E

invece assumiamo una parte tramite bando pubblico, un'altra parte a chiamata a tempo determinato, che non si sa quanto durerà.

E poi parliamo di funzione pubblica ed escludiamo il Ministero per la pubblica amministrazione da tutti gli organismi, sia dal Comitato interministeriale che dal nucleo per la cybersicurezza: la funzione pubblica non c'è.

Mi è stato detto che è un accordo nato così. A me non piace: si parla di funzione pubblica, si parla di uffici pubblici, di sicurezza dello Stato, di enti locali, di parla di sicurezza dei cittadini e il Ministero per la pubblica amministrazione non è previsto all'interno degli organismi. Tutto questo è abbastanza singolare.

L'ultima questione sulla quale voglio spendere il tempo che mi resta è il ruolo del Parlamento.

C'è un articolo all'interno della norma che dice che il Copasir può convocare il direttore generale dell'Agenzia: ma questa è una grande fortuna! Meno male che ce lo dice la legge, meno male.

Signori, in queste settimane, in questi mesi, il Parlamento sta perdendo ogni giorno ruolo, funzione, qualità. Stiamo attenti: non vorrei che prima o poi nascesse un'agenzia parlamentare che ci sostituisse tutti. Rifletteteci. *(Applausi)*.

PRESIDENTE. È iscritto a parlare il senatore Augussori. Ne ha facoltà.

AUGUSSORI *(L-SP-PSd'Az)*. Signor Presidente, userò molto meno del tempo che mi è stato assegnato; sarò molto breve anche perché - è giusto dirlo - questo provvedimento ci arriva dalla Camera dei deputati e, come spesso accade ultimamente, con scarso margine di manovra; quindi, anche l'esame in Commissione è stato abbastanza rapido. È giusto ricordarlo e sottolinearlo tutte le volte perché credo che ribadire ogni volta, indipendentemente dal nostro ruolo di maggioranza o di opposizione, la difesa della centralità del Parlamento sia per noi prima di tutto un dovere.

Dobbiamo però dire che il decreto-legge è uscito dalla Camera praticamente all'unanimità; quindi, possiamo dare seguito in modo rapido ai nostri lavori perché si tratta di un provvedimento fondamentale anche per attuare i nostri impegni legati al PNRR.

È un provvedimento importante per la vera emergenza che - permettetemi - non è esagerato paragonare alla situazione legata al covid. Non si vede, ma da alcuni anni è in corso una vera e propria guerra che non si combatte più sui campi di battaglia, ma lungo le linee di comunicazione informatica. Forse definirla una terza guerra mondiale è esagerato, però è davvero una situazione difficilmente quantificabile e valutabile dai più.

È importante che il Parlamento assuma consapevolezza di ciò che è al giorno d'oggi la cybersicurezza e che si agisca anche perché l'utilizzo di tecnologie informatiche, come è ovvio che sia, aumenta in modo esponenziale di anno in anno. Nell'ultimo anno abbiamo visto quanto tutto ciò che è legato allo *smart working* ci ha portato ad aumentare la diffusione di dati che si muovono lungo le linee telematiche anche in settori che prima ne erano toccati

solo marginalmente e, quindi, la cybersicurezza è un tema centrale della nostra politica. Anche gli attacchi aumentano in modo esponenziale ed è un settore dove - ripeto - l'evoluzione di questi attacchi è sempre crescente.

Volendo fare un paragone, visto che siamo in giornate di eventi sportivi poiché sono in corso i giochi olimpici, direi che dobbiamo agire come l'antidoping che deve seguire il *doping* in continua evoluzione. C'è un *doping* informatico che ogni giorno si evolve e aumenta le proprie capacità e noi dobbiamo inseguire, essere aggiornati e permettere a tutte le amministrazioni pubbliche coinvolte di essere sempre pronte a rispondere a questi attacchi, che mutano giorno dopo giorno.

Non è un tema facile; è un tema delicato, lo sappiamo. Bisogna agire con decisione, ma anche con cautela proprio per la sua delicatezza. Bene ha fatto - rivolgo da parte del nostro Gruppo un plauso ai colleghi dell'altro ramo del Parlamento - la Camera a inserire un maggior coinvolgimento del Parlamento in vari articoli del decreto. È importante che il Parlamento ci sia, venga coinvolto e che in questo modo ci sia anche la possibilità di tenere un rapporto diretto con i cittadini elettori.

L'importanza della cybersicurezza è data anche dall'attualità. Tutti sappiamo che in questi giorni è in corso un attacco *hacker*. Scopriremo i dettagli più avanti, ma possiamo dire che è un attacco informatico fatto per fare male e che ha mostrato le debolezze del nostro sistema, non solo perché vengono trafugati i dati, cosa che già di per sé è grave, ma perché viene compromesso e messo in pericolo l'intervento sulla salute pubblica ed è inutile che vi ripeta quanto ciò sia importante in questo periodo.

Dobbiamo intervenire al più presto per dare strumenti a tutte le nostre istituzioni per affrontare questa sfida. Lo dico anche se avrei potuto - e avrei avuto gioco facile - attaccare la scarsa lungimiranza di quel Presidente di Regione che un anno fa prendeva gli aperitivi sui Navigli. Ce lo ricordiamo, ma non lo voglio fare. Credo che noi, come Gruppo Lega, in quest'Aula dobbiamo dare un segnale diverso, anche se mi domando cosa sarebbe accaduto a parti invertite. *(Applausi)*. Se questo attacco *hacker* avesse colpito non il Lazio, ma un'altra Regione, ad esempio la Lombardia, cosa avremmo ascoltato in quest'Aula oggi? *(Applausi)*. Avremmo ascoltato il senatore Pellegrini chiedere le dimissioni di Fontana? Avremmo sentito il senatore Toninelli chiedere il commissariamento della Regione Lombardia? Sono lontano dalla realtà? No, avremmo sentito queste frasi; avremmo ascoltato, magari dalla sinistra, accuse alla Regione Lombardia di aver messo in pericolo delle vite. Ebbene, l'asteroide caduto a febbraio 2020 sulla testa della Lombardia, oggi sta cadendo sulla Regione Lazio.

Dicevo che avrei gioco facile ad andare avanti per tutti i miei dieci minuti e potrebbero accodarsi tutti i colleghi del Gruppo. Ma noi non vogliamo fare questo e non vogliamo abbassarci a tale livello, e la dimostrazione di questo è la misura del nostro essere qui, il nostro essere in Parlamento e di essere al Governo con responsabilità. *(Applausi)*.

PRESIDENTE. Dichiaro chiusa la discussione generale.

Ha facoltà di parlare la relatrice.

MANTOVANI, *relatrice*. Signor Presidente, farò una breve replica. Sono sicuramente soddisfatta di sentire da tutte le forze politiche che c'è unità e concordia sulla necessità dell'istituzione di questa Agenzia, della cui importanza tutti noi oggi siamo consapevoli. Mi rifaccio a quanto espresso dalla senatrice Tiraboschi sulla necessità di una formazione più pervasiva, in quanto oggi abbiamo una forte carenza di queste professionalità ed è necessario investire fin dalla scuola primaria, anche con una nuova materia scolastica, l'informatica, in modo da avere in futuro più esperti e più professionisti in questo settore.

Per quanto riguarda l'attenzione alle piccole e medie imprese, è necessario un supporto, che verrà da tale Agenzia, e una maggiore interazione tra le necessità di sicurezza delle piccole medie imprese e della pubblica amministrazione. L'Agenzia potrà offrire il supporto necessario a migliorare la sicurezza di tutti.

Una piccola precisazione invece per il senatore Malan, per quanto riguarda i compensi che non spettano al nucleo: il nucleo è un organo consultivo composto dal direttore generale dell'Agenzia, dal consigliere militare del Presidente del Consiglio dei ministri e da alte cariche, che hanno già i propri emolumenti. Per quanto riguarda il personale dell'Agenzia, è previsto all'articolo 12 un trattamento economico pari a quello in godimento da parte dei dipendenti della Banca d'Italia.

PRESIDENTE. Comunico che è pervenuto alla Presidenza - ed è in distribuzione - il parere espresso dalla 5ª Commissione permanente sul disegno di legge in esame, che verrà pubblicato in allegato al Resoconto della seduta odierna.

Passiamo all'esame dell'articolo 1 del disegno di legge.

Avverto che gli ordini del giorno si intendono riferiti agli articoli del decreto-legge da convertire, nel testo comprendente le modificazioni apportate dalla Camera dei deputati.

Procediamo all'esame degli ordini del giorno riferiti all'articolo 4 del decreto-legge, che si intendono illustrati e su cui invito la relatrice e il rappresentante del Governo a pronunziarsi.

MANTOVANI, *relatrice*. Signor Presidente, esprimo parere favorevole all'accoglimento dell'ordine del giorno G4.100. Il parere è favorevole anche sull'ordine del giorno G4.101, a condizione che venga espunto il secondo paragrafo. Invito al ritiro dei restanti ordini del giorno, altrimenti il parere è contrario.

D'INCÀ, *ministro per i rapporti con il Parlamento*. Signor Presidente, esprimo parere conforme a quello della relatrice.

PRESIDENTE. Essendo stato accolto dal Governo, l'ordine del giorno G4.100 non verrà posto ai voti.

Senatrice Rauti, concorda con la riformulazione dell'ordine del giorno G4.101, proposta dalla relatrice?

RAUTI *(FdI)*. Sì, signor Presidente.

PRESIDENTE. Essendo stato accolto dal Governo, l'ordine del giorno G4.101 (testo 2) non verrà posto ai voti.

C'è un invito al ritiro degli ordini del giorno da G4.102 a G4.105, altrimenti il parere è contrario. Senatore Mallegni, intende ritirarli?

MALLEGNI *(FIBP-UDC)*. Sì, signor Presidente, li ritiro.

PRESIDENTE. Passiamo all'esame dell'ordine del giorno riferito all'articolo 5 del decreto-legge, che si intende illustrato e su cui invito la relatrice e il rappresentante del Governo a pronunziarsi.

MANTOVANI, *relatrice*. Signor Presidente, invito al ritiro dell'ordine del giorno G5.100, altrimenti il parere è contrario.

D'INCÀ, *ministro per i rapporti con il Parlamento*. Signor Presidente, esprimo parere conforme a quello della relatrice.

PRESIDENTE. Senatore Mallegni, intende ritirare l'ordine del giorno G5.100?

MALLEGNI *(FIBP-UDC)*. Sì, signor Presidente, lo ritiro.

PRESIDENTE. Passiamo all'esame dell'ordine del giorno riferito all'articolo 6 del decreto-legge, che invito i presentatori ad illustrare.

MALLEGNI *(FIBP-UDC)*. Signor Presidente, ritiro l'ordine del giorno G6.100.

PRESIDENTE. Passiamo all'esame degli ordini del giorno riferiti all'articolo 7 del decreto-legge, che si intendono illustrati e su cui invito la relatrice e il rappresentante del Governo a pronunziarsi.

MANTOVANI, *relatrice*. Signor Presidente, invito al ritiro dell'ordine del giorno G7.100, altrimenti il parere è contrario.

Esprimo parere favorevole all'accoglimento degli ordini del giorno G7.101, G7.102, G7.103, G7.104 e G7.105 (testo 2).

D'INCÀ, *ministro per i rapporti con il Parlamento*. Signor Presidente, esprimo parere conforme a quello della relatrice.

PRESIDENTE. C'è dunque un invito al ritiro dell'ordine del giorno G7.100, presentato dal senatore Marilotti.

D'ARIENZO *(PD)*. Domando di parlare.

PRESIDENTE. Ne ha facoltà.

D'ARIENZO *(PD)*. Signor Presidente, vista l'assenza del senatore Marilotti, faccio mio l'ordine del giorno G7.100 e lo ritiro.

PRESIDENTE. Essendo stati accolti dal Governo, gli ordini del giorno G7.101, G7.102, G7.103, G7.104 e G7.105 (testo 2) non verranno posti ai voti.

Passiamo all'esame degli ordini del giorno riferiti all'articolo 10 del decreto-legge, che si intendono illustrati e su cui invito la relatrice e il rappresentante del Governo a pronunziarsi.

MANTOVANI, *relatrice*. Signor Presidente, esprimo parere favorevole all'accoglimento dell'ordine del giorno G10.100, purché alla fine dell'impegno sia inserita la formula «compatibilmente con gli equilibri di finanza pubblica».

Esprimo parere favorevole sugli ordini del giorno G10.101 e G10.102. Esprimo parere favorevole sull'ordine del giorno G10.103, a condizione che nell'impegno siano espunte le parole "l'obbligo" e che conseguentemente il testo sia riformulato in modo corretto grammaticalmente: «valutare l'opportunità di prevedere, per imprese operanti in settori strategici e pubblica amministrazione, l'adozione di strumenti (...)». Esprimo parere favorevole sull'ordine del giorno G10.104. Esprimo parere favorevole sull'ordine del giorno G10.105, a condizione che nell'impegno sia inserita la formulazione: «compatibilmente con gli equilibri di finanza pubblica».

D'INCÀ, *ministro per i rapporti con il Parlamento*. Signor Presidente, esprimo parere conforme a quello della relatrice.

PRESIDENTE. Senatrice Rauti, accetta la riformulazione dell'ordine del giorno G10.100?

RAUTI *(FdI)*. Sì, signor Presidente.

PRESIDENTE. Essendo stati accolti dal Governo, gli ordini del giorno G10.100 (testo 2), G10.101 e G10.102 non verranno posti ai voti.

Senatrice Rauti, accetta la riformulazione dell'ordine del giorno G10.103?

RAUTI *(FdI)*. Sì, signor Presidente.

PRESIDENTE. Essendo stati accolti dal Governo, gli ordini del giorno G10.103 (testo 2) e G10.104 non verranno posti ai voti.

Senatrice Binetti, accetta la riformulazione dell'ordine del giorno G10.105?

BINETTI *(FIBP-UDC)*. Sì, signor Presidente.

PRESIDENTE. Essendo stato accolto dal Governo, l'ordine del giorno G10.105 (testo 2) non verrà posto ai voti.

Passiamo all'esame dell'ordine del giorno riferito all'articolo 11 del decreto-legge, che si intende illustrato e su cui invito la relatrice e il rappresentante del Governo a pronunziarsi.

MANTOVANI, *relatrice*. Signor Presidente, sull'ordine del giorno G11.100 formulo un invito al ritiro o altrimenti esprimo parere contrario.

PRESIDENTE. Senatore Mallegni, accoglie l'invito al ritiro formulato dalla relatrice?

MALLEGNI *(FIBP-UDC)*. Signor Presidente, ritiro l'ordine del giorno G11.100.

PRESIDENTE. Passiamo all'esame dell'ordine del giorno riferito all'articolo 12 del decreto-legge, che si intende illustrato e su cui invito la relatrice e il rappresentante del Governo a pronunziarsi.

MANTOVANI, *relatrice*. Signor Presidente, sull'ordine del giorno G12.100 formulo un invito al ritiro o altrimenti esprimo parere contrario.

D'INCÀ, *ministro per i rapporti con il Parlamento*. Signor Presidente, esprimo parere conforme a quello della relatrice.

PRESIDENTE. Senatore Mallegni, accoglie l'invito al ritiro formulato dalla relatrice?

MALLEGNI *(FIBP-UDC)*. Signor Presidente, ritiro l'ordine del giorno G12.100.

PRESIDENTE. Passiamo alla votazione finale.

GARAVINI *(IV-PSI)*. Domando di parlare per dichiarazione di voto.

PRESIDENTE. Ne ha facoltà.

GARAVINI *(IV-PSI)*. Signor Presidente, onorevoli colleghi, l'assoluta impossibilità di prenotare ogni tipo di visita medica, incluse le vaccinazioni anti-Covid, il sito della Regione irraggiungibile per giorni e i dati di tutti gli utenti in balia di criminali sconosciuti, interessati solo a richiedere chissà quale tipo di riscatto. L'attacco *hacker* di questi giorni al sistema sanitario della Regione Lazio è la dimostrazione plastica di quanto sia urgente definire una politica nazionale di sicurezza cibernetica, anche perché l'esperienza insegna che le incursioni cibernetiche ad un Paese colpiscono frequentemente aspetti nevralgici del Paese stesso (sistemi aeroportuali, banche, turbine elettriche), come pure grandi aziende del settore privato, bloccate nella loro operatività e messe sotto ricatto attraverso estorsioni milionarie.

È recente, ad esempio, il caso della manipolazione telematica a danno della più grande catena di supermercati svedese, costretta a chiudere per giorni oltre 800 punti vendita. Oppure l'attacco *hacker* da parte del gruppo russo Revil a migliaia di aziende statunitensi, che ha mandato in *tilt* decine di migliaia di *computer* in tutto il mondo. Sono esempi calzanti, che fanno capire quanto sia necessario che anche il nostro Paese si doti di uno strumento idoneo a proteggere le funzioni essenziali dello Stato da minacce informatiche, alzando il livello di protezione dei dati e dei sistemi di controllo.

Ad oggi si stima che le imprese italiane subiscano ogni anno mediamente 7 miliardi di euro di danni a causa di attentati digitali e solo poche settimane fa abbiamo appreso con sgomento dalle parole del ministro Colao che almeno il 95 per cento delle piattaforme di cui si serve la nostra pubblica amministrazione non è in sicurezza. Ecco perché la realizzazione di un'Agenzia per la *cybersecurity* non è più rinviabile. C'è bisogno urgentemente di dotarsi di uno strumento efficace, che difenda i comparti strategici della nostra sicurezza nazionale dai pericoli rappresentati dalla crescente pirateria informatica, così da tutelarci da possibili aggressioni provenienti da altri Paesi o da forze destabilizzanti e antidemocratiche.

L'Agenzia per la cybersicurezza deve rispondere a due missioni principali: innanzitutto alla cosiddetta cyber-resilienza, cioè il consolidamento della collaborazione ai fini della sicurezza cibernetica con l'insieme degli operatori strategici che operano nel settore delle telecomunicazioni, dell'energia, dei trasporti, della difesa, dello spazio e dell'economia, dalla cui integrità dipende il funzionamento del sistema Paese. In secondo luogo, l'Agenzia dovrà fungere da centro di coordinamento nazionale per gli investimenti nella sicurezza cibernetica.

In sostanza, possiamo contare su un organismo in grado di connettere aziende piccole e grandi, capace di coinvolgere le università e la ricerca e di potenziare l'industria del settore rendendola impermeabile ad infiltrazioni ostili, anche da parte di Paesi stranieri.

L'Agenzia che andiamo ad istituire con il voto odierno evita la sovrapposizione di compiti con il comparto *dell'intelligence*; è collocata sotto la diretta responsabilità del Presidente del Consiglio, di conseguenza non è soggetta necessariamente a vincoli di segretezza. Diventa un organismo rapido, snello, adeguato alla complessità della sfida, in grado di svolgere una copertura a 360 gradi ed è virtuoso, perché prevede una *partnership* strutturata e continua tra soggetti pubblici e privati, che lavorano assieme nell'ambito di un'autentica strategia nazionale di sicurezza.

Inoltre, la creazione di un'Agenzia nazionale avrà effetti positivi anche dal punto di vista economico; infatti, proteggendo in maniera efficace il nostro spazio cibernetico, rendiamo l'Italia più attraente anche per investitori nazionali e stranieri. È il caso di dire quindi che la ripartenza dell'Italia passa anche da qui, da un'Agenzia nazionale in grado di mettere in sicurezza il Paese anche sotto il profilo cibernetico.

Noi siamo fortemente convinti della necessità di accelerare i processi di digitalizzazione della società e della pubblica amministrazione, allo scopo di modernizzare il Paese; al tempo stesso siamo consapevoli dei forti rischi legati a possibili attacchi informatici alle istituzioni e ai singoli. Per di più la

nostra pubblica amministrazione è in procinto di spostare tutti i propri dati su un *cloud* nazionale, vale a dire su uno spazio di stoccaggio digitale che ci espone ad ulteriori, possibili attacchi. Pertanto, la necessità di tutelare il Paese dalla minaccia cibernetica è uno dei *dossier* più delicati, per noi come per ogni moderna democrazia.

Si tratta di una questione di sicurezza nazionale e, al tempo stesso, anche di politica estera. Ci troviamo, infatti, in una fase storica nella quale diversi Paesi, dalla Russia alla Cina, mirano ad acquisire un vantaggio geopolitico attraverso la loro supremazia tecnologica. Un tempo la geopolitica aveva un notevole influsso sulla tecnologia, oggi accade il contrario: la capacità di dotarsi di tecnologie innovative attribuisce un vantaggio strategico in termini di esercizio del potere. Basta guardare quale effetto sta avendo sugli equilibri internazionali il predominio cinese del 5G, cioè la nuova rete digitale di quinta generazione di supporto alla telefonia mobile. Questo è il motivo per cui occorre porre un'attenzione particolare al concetto di sovranità tecnologica ed è necessario che ci allineiamo in fretta all'interno dell'Unione europea, così da colmare il ritardo esistente in materia di nuove tecnologie e dotarci di una vera e propria sovranità tecnologica a livello europeo, che ci permetta di tutelare i nostri commerci, la nostra economia e i nostri valori e che determini la nostra autonomia strategica, vale a dire la possibilità di intervenire da soli per fronteggiare possibili aggressioni.

Gli attacchi cibernetici sono una minaccia potenzialmente letale per ogni sistema democratico, perché rischiano di mettere in ginocchio settori essenziali di un Paese: centrali elettriche, rifornimenti idrici, discariche di rifiuti; in altre parole, tutti i sistemi vitali di un Paese. Per questo serve una visione comune in materia di cyberdifesa a livello nazionale ed europeo: esattamente ciò che cerchiamo di fare con questo decreto-legge, col quale ci adeguiamo agli *standard* europei e ci dotiamo di una sorta di scudo di difesa dalle aggressioni digitali. Contemporaneamente, mandiamo anche un messaggio all'esterno, a quei Paesi dai quali provengono gran parte degli attacchi cibernetici. Diciamo forte e chiaro che l'Italia è fermamente determinata a non lasciarsi mettere sotto scacco.

In sostanza, signor Presidente, la tecnologia sta cambiando passo: porta con sé vantaggi, ma anche rischi, ed è necessario che ci attrezziamo di conseguenza, anche e soprattutto in una fase come quella attuale, in cui si realizza una profonda interrelazione tra la nostra quotidianità e l'informatica. Via via stiamo affidando gran parte della nostra stessa esistenza alla tecnologia: abbiamo un'identità digitale con la quale possiamo accedere a tutta una serie di servizi dal nostro pc. Possiamo ormai fare di tutto con il nostro cellulare, tante nostre informazioni delicate e sensibili sono contenute all'interno di sistemi informatici complessi, così che i dati personali di un soggetto sono sempre più appetibili, purtroppo anche per *hacker* e criminali informatici.

Questo è il motivo per cui la sicurezza cibernetica e la tutela dei dati non sono più soltanto un concetto astratto, ma riguardano la vita di tutti noi, il nostro quotidiano. La società tutta sta subendo profondi cambiamenti: grandi istituzioni come la scuola, il Servizio sanitario nazionale, la pubblica amministrazione, come pure il mondo economico produttivo, negli ultimi anni stanno ricorrendo sempre più frequentemente al digitale, dallo *smart*

working al *green pass*, dalla didattica a distanza alla telemedicina, tutti strumenti di grande utilità, che allo stesso tempo però ci espongono a rischi finora inimmaginabili.

Ecco perché c'è bisogno di strumenti di protezione adeguati come l'Agenzia nazionale per la sicurezza cibernetica, che rappresenta un nuovo tassello di quell'Italia che stiamo costruendo con il Governo Draghi, moderna ed efficiente, che punta all'innovazione e alle nuove tecnologie, ma capace al tempo stesso di tutelare i diritti delle cittadine e dei cittadini, cosicché l'Italia del domani inizi già oggi. *(Applausi)*.

RAUTI *(FdI)*. Domando di parlare per dichiarazione di voto.

PRESIDENTE. Ne ha facoltà.

RAUTI *(FdI)*. Signor Presidente, onorevoli colleghi e rappresentanti del Governo, quando si dice il caso o il destino: è singolare che oggi affrontiamo un provvedimento sull'architettura nazionale, sulla cybersicurezza e sull'istituzione dell'Agenzia per la sicurezza nazionale e la coincidenza vuole che questo accada dopo un attacco *cyber* al Centro elaborazione dati (CED) del Lazio, che ha mandato in tilt la sanità della Regione.

Partiamo dalla cronaca per andare oltre: voglio sottolineare che fino al 13 agosto non si potranno prenotare altri vaccini negli *hub* del Lazio, mentre la mannaia del *green pass* del 6 agosto è davanti a noi e si sta per abbattere su tutti quelli che sono in partenza; e non sappiamo se è solo l'inizio. *(Applausi)*. Basta leggere i giornali di oggi: la paura, il silenzio e l'idea che ci sia un ricatto. Insomma, non sappiamo se è solo l'inizio e se questo attacco vuole arrivare ad altro e colpire altri obiettivi più ampi o se è la sanità il vero obiettivo; chi lo sa.

Sicuramente la situazione è seria - non da oggi - ed è necessaria - non da oggi - l'istituzione dell'Agenzia per la cybersicurezza.

Noi di Fratelli d'Italia siano consapevoli che ciò rappresenti solo il primo passo e da tre anni - sia alla Camera dei deputati, sia al Senato - con tutti gli strumenti a disposizione, abbiamo chiesto l'istituzione di quest'Agenzia, oltre a una strategia organica sulla *cybersecurity* e a un rafforzamento cibernetico in vari settori (sanitario, produttivo, industriale e della pubblica amministrazione) anche per i singoli cittadini, che sono tutti utenti del cyberspazio.

Pertanto, molto prima che nel contesto del PNRR si inserisse il tema della transizione digitale, Fratelli d'Italia chiedeva, con tutti gli strumenti a disposizione, l'istituzione dell'Agenzia e sottolineava la necessità di reti resilienti. Abbiamo denunciato più volte il ritardo accumulato su questo fronte e la necessità di una garanzia di sicurezza nazionale finalizzata alla sovranità digitale.

È dal settembre 2020 che il Governo ha assunto un impegno che non ha mantenuto. Ci siamo trascinati fin qui con un ritardo colpevole, ingiustificabile e grave, anche perché - com'è noto - con la crescita delle reti è aumentato anche il rischio di violazioni e quindi il dominio *cyber* (la cosiddetta

quinta dimensione) è diventato la nuova frontiera e la linea di confronto a livello geopolitico.

Cari colleghi, non vi sfuggirà che esplorare lo spazio cibernetico significa entrare in un teatro operativo. Dopo i domini tradizionali (aria, terra e mare) si sono aggiunti il quarto (spazio) e il quinto (*cyber)*, che decide della sicurezza globale.

Non è un caso se nell'ultimo vertice NATO, in cui è stata approvata la nuova *cyber defense policy*, la minaccia cibernetica è stata equiparata ad altre tipologie di attacco sufficienti per attivare il famoso articolo 5 del Trattato, che coinvolge anche gli altri Paesi alleati a intervenire.

È evidente a tutti che siamo in un mondo sempre più interconnesso non soltanto a causa della pandemia e che questo aumento determina un'impennata dei rischi di hackeraggio e una minaccia di attacchi *cyber* sempre più sofisticati e con vari obiettivi, come sottrarre dati per fini predatori e rubare la proprietà intellettuale e l'identità, ma anche - attenzione - obiettivi molto più ambiziosi, come per esempio manipolare informazioni, danneggiare infrastrutture e bloccare erogazioni di servizio, per non parlare del proselitismo dei radicali violenti che si fa *online* e dello spionaggio industriale e militare. Questa è la vera trincea.

Evidentemente, non è bastato quanto contenuto nella relazione annuale dei nostri Servizi, in cui si è sottolineata la criticità nella sicurezza informatica. Sono ormai note la vulnerabilità e la permeabilità delle reti e, quando si diceva ciò, contestualmente aumentavano gli attacchi *cyber* in termini sia qualitativi, sia quantitativi.

Ricordo anche l'allarme lanciato, non da ultimo, dal ministro Colao, che ha detto che oltre il 95 per cento dei *server* della pubblica amministrazione è obsoleto e a rischio. Lo ripeto: oltre il 95 per cento. C'è stata anche un'impennata di attacchi tra il 2009 e il 2020. Ma chi li conta? Li ha contati il Governo? No.

Oggi tutti piangiamo per quanto è successo ai danni della Regione Lazio, ma ci pare un po' tardi per stracciarsi le vesti, perché il tema della sicurezza nazionale non nasce oggi, ma è un'emergenza che si è imposta da tempo. L'Agenzia dedicata era una necessità e un'opportunità ineludibile, che arriva in ritardo: non c'è niente di più opportuno e niente di più tardivo. *(Applausi)*.

Questo è il punto. È questa la colpa che vi imputiamo oggi, perché i Governi ci hanno portato fin qui e non ci potete accusare di ostruzionismo. Siamo stati collaborativi e propositivi - sono appena stati accolti più di dieci ordini del giorno di Fratelli d'Italia - però è imperdonabile il ritardo colpevole con il quale nasce l'Agenzia.

Perché questo ritardo? Qualcosa la voglio e la devo ricordare a chi magari ha la memoria corta. Oggi infatti tutti prendiamo consapevolezza che c'è un rischio *cyber*, ma lo sapevamo già e lo sapevamo bene.

Voglio rammentare che la direttiva europea è del 2016 e che nel 2017 l'Italia annunciò l'istituzione dell'Agenzia, che però non ci fu. Voglio sottolineare che nella bozza della legge di bilancio comparve a un certo punto l'Agenzia, che poi nella versione definitiva è scomparsa. Ricordate che interrogammo anche il Ministro competente? Ricordate che questo argomento è stato uno dei tre cardini su cui è caduto il Governo Conte II? Memoria corta,

memoria corta *(Applausi)*, ma noi ve la rinfreschiamo, perché il ritardo è vostro ed è una colpa grave, soprattutto oggi.

Questi ritardi sono vostri, sono una responsabilità, perché stiamo parlando di attacchi che possono comportare il collasso di un sistema; stiamo parlando della nuova sfida sistemica e di *asset* fondamentali. Qui la sfida non è soltanto la prenotazione dei vaccini, pur importantissima; qui la sfida è geopolitica, è geostrategica.

Cari colleghi, caro rappresentante del Governo, la nostra astensione è dunque una lezione al vostro ritardo colpevole, non è certo mettere in dubbio la validità, la necessità, l'urgenza e l'importanza di quest'Agenzia.

Attenzione, però, perché la sfida è alta e importante e non si risponde a una sfida strategica con un carrozzone politico. Quindi fate l'Agenzia: fatela subito, fatela bene e fatela funzionare. In ogni caso, il ritardo con il quale arriviamo oggi qui è vostro ed è una responsabilità da cui nessuno vi potrà assolvere. *(Applausi)*.

PINOTTI *(PD)*. Domando di parlare per dichiarazione di voto.

PRESIDENTE. Ne ha facoltà.

PINOTTI *(PD)*. Signor Presidente, l'hackeraggio dei dati sanitari della Regione Lazio pone questa nostra discussione in una situazione di drammatica e stretta attualità. Lo hanno notato alcuni colleghi e non c'è dubbio, quindi, che il Parlamento stia parlando di qualcosa cui il Paese guarda con estrema attenzione e preoccupazione.

Che sia necessario correre sulle decisioni che riguardano la cybersicurezza lo stanno dicendo in molti in questi giorni. Lo ha detto l'Autorità delegata in una recente intervista, così come ha fatto in una dichiarazione anche il presidente Zingaretti e qui mi permetto di aprire e chiudere una parentesi. Credo che non mi abbiate mai sentito in quest'Aula dire una parola di polemica sul Covid-19 o sulle situazioni che lo riguardano: non l'ho fatto mai per scelta; non perché a volte non potesse essere utile farlo, ma non l'ho fatto. Che oggi, dunque, su un decreto di questa urgenza, su un fatto che potrebbe capitare a chiunque - chi ha capito come funzionano gli attacchi *cyber*, infatti, comprende che il punto debole della rete potrebbe essere di chiunque - si parli per farne una questione di polemica politica, e mi rivolgo al collega Augussori, francamente non mi pare all'altezza della questione. *(Applausi)*.

Questa esigenza di correre, signor Presidente, non è che il Parlamento non l'avesse recepita già prima. In Commissione difesa abbiamo recentemente concluso un'indagine conoscitiva molto approfondita proprio sui temi relativi al mondo cyber. Siamo partiti dai profili riguardanti la difesa e la sicurezza, però ci siamo allargati - com'è ovvio per questa materia - agli affari esteri, al Ministero degli interni e al Ministero della ricerca. Abbiamo udito poi anche grandi aziende, perché il problema non riguarda soltanto il settore pubblico. Ne è emerso, signor Presidente, un quadro di grande allarme.

Nelle audizioni che abbiamo svolto, è stato evidenziato l'aumento esponenziale degli attacchi cyber, ulteriormente incrementati nel periodo Covid, per lo *smart working* e per le situazioni che si stavano creando. I dati

sono impressionanti. Il tema legato al rischio dei dati sanitari, che oggi stiamo mettendo in evidenza per quello che riguarda la Regione Lazio, in Commissione difesa era già stato sottolineato dalla dottoressa Nunzia Ciardi, direttrice del servizio della Polizia postale, che ha fatto un'audizione brillantissima, molto interessante. Oltre a mettere in evidenza l'aumento dei crimini, ci ha raccontato la storia - che oggi sta riemergendo - di una donna tedesca, morta perché un attacco *cyber* ha bloccato di fatto un ospedale e, quando è giunta al pronto soccorso, non sono potuti intervenire, ma lei non aveva il tempo di arrivare in un altro ospedale. Stiamo quindi parlando di rischi non solo per le risorse e per l'economia, ma per la vita: questa è la gravità della situazione.

È stato ricordato, inoltre, che anche l'Irlanda ha subito un attacco al sistema sanitario, proprio perché il tema della sanità, così importante per ciascuno di noi, diventa un elemento particolarmente sensibile.

Al termine del lavoro svolto in Commissione, è stata votata all'unanimità una risoluzione finale che ha messo in evidenza una serie di impegni, che riguardano la Difesa e l'esigenza dei collegamenti internazionali, e ha messo a punto, come indirizzi al Governo, alcune delle questioni oggi al nostro esame, tra le quali l'esigenza di avere un'Autorità unica, debba occuparsi dei servizi pubblici, ma anche dei privati, e quella di formazione e di personale altamente qualificato, perché stiamo parlando di una materia con un'evoluzione così rapida che, se non stiamo al passo con i tempi, i cosiddetti cattivi diventano molto più forti di noi.

Da questo punto di vista, è importante che oggi arrivi in Senato un provvedimento su cui ha lavorato molto la Camera. Sono d'accordo con i giudizi positivi che ho ascoltato da parte di molti colleghi sui miglioramenti apportati alla Camera, sia specificando i confini dell'Agenzia, sia ampliando il ruolo del Parlamento. Oggettivamente, però, il Senato ha un avuto un tempo molto ridotto per trattare il tema al nostro esame. È stato importante, comunque, che in Commissione tale approfondimento ci sia stato.

L'Agenzia ha una personalità giuridica di diritto pubblico, è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, ed avrà il compito di svolgere il ruolo di Autorità nazionale, come ricordava prima un collega di Forza Italia, attuando una centralizzazione delle funzioni e delle competenze che finora erano distribuite fra enti e Ministeri: questa era la principale fragilità, perché è necessaria una risposta unitaria e le risposte non possono essere frammentate.

Nell'audizione dell'Autorità delegata, che si è tenuta alla Camera, il sottosegretario Gabrielli ha ricordato - e alcuni interventi lo hanno rilevato - come in realtà la Germania si sia mossa già nel 1991, creando un'Agenzia che oggi dispone di 1.200 unità di personale. In Francia, un'Agenzia simile è nata nel 2009. Lo dico perché ho sentito anche la collega Rauti dire che è tutta colpa del Governo, o comunque degli ultimi Governi. Ricordo che dal 1991 ad oggi si sono succeduti Governi di cui hanno fatto parte anche esponenti che oggi sono in Fratelli d'Italia. Lo dico perché, se vogliamo affrontare con serietà questi argomenti, visto che poi voteremo quasi all'unanimità, con alcune astensioni, forse sarebbe bene evitare i distinguo politici, altrimenti non riusciamo a capire davvero bene la materia.

A questo punto, è stata identificata l'esigenza di avere un'unica autorità. All'inizio era stata individuata l'Autorità militare alla Presidenza del Consiglio, poi si è pensato al Dipartimento delle informazioni per la sicurezza (DIS). Oggi finalmente si individua lo strumento che considero corretto, perché c'è bisogno di avere un'agenzia che crei *software* e *hardware,* ma che sia un punto di riferimento sia per il pubblico sia per il privato. Da questo punto di vista, il tipo di strutturazione che si dà a quest'agenzia mi convince molto, perché i problemi che erano sorti in una prima ipotesi nel Governo precedente e che sembravano non delineare bene i confini fra le Agenzie di *intelligence* e il ruolo di questa adesso sono chiariti: l'*intelligence* fa l'*intelligence,* continua i propri compiti; è chiaro che si interfaccia con l'Agenzia - come faranno il Ministero della difesa e quello dell'interno - che però ha un altro ruolo, compreso quello importantissimo della produzione di strumenti. Infatti, se vogliamo che su questo tema l'Italia sia sicura, deve avere anche una capacità di produzione autonoma di sistemi.

Il ministro Colao - e vedo qui la Sottosegretaria per questi temi - si dice preoccupato perché il 95 per cento delle pubbliche amministrazioni è molto debole da questo punto di vista e dice che sta lavorando sul *cloud,* rispetto al quale è importante utilizzare le migliori tecnologie, che in questo momento non sono italiane, le cui chiavi di utilizzo devono essere però nazionali. Con queste affermazioni fa una scelta importantissima, però dobbiamo implementarla con produzioni, capacità e quindi sviluppi anche industriali nazionali. L'Agenzia ha anche questa funzione, oltre a quella di essere il punto in cui arrivano gli allarmi degli attacchi, che prima erano al Ministero dello sviluppo economico (Mise), con una dotazione di personale estremamente ridotta, mentre ora ci sarà la possibilità di implementarla significativamente.

Questo è un tema cruciale per il futuro di qualsiasi Paese e per la sicurezza dell'economia, dello sviluppo, della crescita, ma anche della vita, come ha dimostrato la storia di quella povera signora tedesca. Il cambiamento culturale che dobbiamo fare è fondamentale, perché, quando riceviamo un attacco, siamo già in ritardo. Il tema vero della cybersicurezza è infatti come prevenire e riguarda la *safety* più che la *security,* perché abbiamo bisogno di prevenire. Quando si parla di sicurezza, è sempre importante prevenire; lo è anche per le Forze armate, ma per la cybersicurezza diventa fondamentale, perché, quando si apre un varco, il rischio diventa veramente generalizzato.

Presidenza del vice presidente LA RUSSA (ore 18,43)

(*Segue* PINOTTI). Concludo il mio intervento dicendo che votiamo convintamente a favore del provvedimento, persuasi che questo strumento sia importante, ma sapendo anche che è l'inizio di una *road map* che deve prevedere la messa in sicurezza della pubblica amministrazione, l'educazione e la formazione (perché dalla scuola è importante che si capiscano i rischi), gli investimenti, le assunzioni, le collaborazioni internazionali e anche l'adeguamento del quadro politico e giuridico nazionale e internazionale. Il tema, in-

fatti, sarà anche come si perseguono questi reati quando gli *hacker* sono stranieri non identificati, che però producono danni terrificanti all'economia o alla sicurezza di una Nazione.

Abbiamo quindi davanti un percorso che comincia, ma certo non finisce con oggi; oggi però decidiamo qualcosa che è necessario e importante. *(Applausi)*.

RUOTOLO *(Misto-LeU-Eco)*. Domando di parlare per dichiarazione di voto.

PRESIDENTE. Ne ha facoltà.

RUOTOLO *(Misto-LeU-Eco)*. Signor Presidente, rappresentanti del Governo, colleghe e colleghi, finalmente stiamo per licenziare questo provvedimento. I fatti di queste ultime ore ci dicono che siamo arrivati in ritardo e che le polemiche nei confronti dell'ex presidente Conte erano pretestuose, perché era stato proprio lui a proporre un ragionamento serio su queste questioni. I fatti di queste ore ci dicono anche che dobbiamo rapidamente recuperare il tempo perso e rendere operativa l'Agenzia per la cybersicurezza nazionale.

Colleghe e colleghi, era già scritto purtroppo. Sono andato a rileggere le pagine di un libro, «Guerra senza limiti. L'arte della guerra asimmetrica fra terrorismo e globalizzazione», scritto sul finire degli anni Novanta da due colonnelli cinesi commissari politici dell'esercito cinese - la prefazione in italiano è del generale Fabio Mini - che avevano previsto attentati come quello alle Torri Gemelle, analizzando i nuovi scenari bellici in chiave di guerre asimmetriche e spiegando il terrorismo e le sue tecniche; le guerre asimmetriche vengono condotte attraverso la manipolazione dei *media*, le turbative dei mercati azionari, la diffusione di virus informatici, le azioni di pirateria sul *web* e la manipolazione del voto. Oggi prendiamo drammaticamente atto di questi nuovi scenari bellici.

Capisco il presidente della Regione Lazio, Nicola Zingaretti, quando afferma che l'attacco informatico nel sistema virtuale gestito da LAZIOcrea è un atto di terrorismo. Sì, è terrorismo, anche se i pirati informatici hanno chiesto il riscatto. Pensiamo agli effetti provocati, al blocco totale delle prenotazioni vaccinali e alle visite in ospedale nelle ASL che sono ferme; il sistema serve anche per la gestione degli appalti e del pagamento del bollo per i veicoli e delle tasse regionali. Se fino a qualche tempo fa gli *hacker* rubavano segreti aziendali per ricatto, estorsione o per rivenderli ai concorrenti, quello che è certo è che la digitalizzazione ha avuto una forte accelerazione con la pandemia e quindi oggi mettere in sicurezza i dati è assolutamente fondamentale per la sicurezza del Paese. Sotto attacco possono finire tutti gli enti, quelli istituzionali innanzitutto, aziende pubbliche e private. Dopo l'attacco *hacker* alla Regione Lazio, infatti, l'antiterrorismo teme che altri siti istituzionali possano essere violati.

Nel 2020 - ci dicono gli esperti - ci sono stati 156 episodi di *cybercrime* o di cyberspionaggio al mese; quest'anno attacchi informatici hanno bloccato ospedali, gasdotti e impianti di purificazione dell'acqua in città.

Quanto sta accadendo nel Lazio è la dimostrazione plastica di quanto sia importante che lo Stato approntì le migliori soluzioni possibili per scongiurare il verificarsi di episodi simili. La vulnerabilità dei sistemi informatici è un rischio che la pubblica amministrazione non può permettersi di correre, perché la assoggetterebbe al pericolo del rallentamento, quando non di una vera e propria paralisi dell'azione amministrativa, e inoltre può essere fonte di danni rilevantissimi sul fronte della violazione di dati personali e della loro divulgazione o mercificazione.

L'emergenza Covid ha poi dimostrato che un uso maggiore degli strumenti informatici e delle connessioni in rete amplifica le occasioni di attacco. Come si legge nella relazione sulla politica dell'informazione per la sicurezza 2020, la pandemia è stato un evento determinante anche in termini di impatto sulla società, sulle tecnologie in uso alla popolazione, sulla digitalizzazione di attività e servizi, nonché sul conseguente ampliarsi della superficie di rischio cibernetico per l'individuo e per l'intero sistema Paese. Hanno quindi acquisito maggiore attualità e concretezza le minacce alla sicurezza e al funzionamento delle reti e degli impianti, nonché alla continuità degli approvvigionamenti. Nel complesso, si è evidenziato come gli attori ostili abbiano sfruttato nel periodo pandemico il massiccio ricorso al lavoro agile e la conseguente accessibilità da Internet di risorse digitali di Ministeri e aziende di profilo strategico e infrastrutture critiche, divenuti ancor più bersaglio di campagne ostili.

Colleghe e colleghi, la sicurezza cibernetica costituisce uno degli interventi previsti dal Piano nazionale di ripresa e resilienza trasmesso dal Governo alla Commissione europea il 30 aprile 2021 e definitivamente approvato il 13 luglio 2021.

In particolare, in tale ambito, la *cybersecurity* è uno dei sette investimenti della digitalizzazione della pubblica amministrazione.

Avete sentito la collega Pinotti ricordare le dichiarazioni del ministro Colao: il 95 per cento dei *server* della pubblica amministrazione non è sicuro. È vero, bisogna correre. Abbiamo bisogno di sviluppare in tempi brevi, idonei e sempre più serrati meccanismi di tutela.

Altri Paesi hanno investito nella sicurezza informatica da anni, come la Francia e la Germania. Appare quindi urgente intervenire rinforzando il sistema di difesa contro questo genere di reati, che possono rivelarsi particolarmente insidiosi e creare danni ingenti.

L'istituzione dell'Agenzia nazionale per la cybersicurezza, del Comitato interministeriale per la cybersicurezza e, nell'ambito di quest'ultimo, del nucleo per la cybersicurezza sembra essere un passo in avanti nell'ammodernamento del sistema di sicurezza nazionale.

Per questo motivo, dichiaro il voto a favore delle senatrici e dei senatori di Liberi e Uguali-Ecosolidali. *(Applausi)*.

GASPARRI *(FIBP-UDC)*. Domando di parlare per dichiarazione di voto.

PRESIDENTE. Ne ha facoltà.

GASPARRI *(FIBP-UDC)*. Signor Presidente, il Gruppo Forza Italia voterà a favore di questo provvedimento e ovviamente aggiungiamo anche noi alcune considerazioni rispetto alla vicenda.

In un libro pubblicato recentemente in occasione dei quarant'anni dall'insediamento di Ronald Reagan alla Casa Bianca, una biografia del Presidente americano scritta dal giornalista Gennaro Sangiuliano, uno dei capitoli finali parla della vittoria nella Terza guerra mondiale, che è stata attribuita a Reagan. Qualcuno si potrebbe chiedere quale sia stata questa Terza guerra mondiale. Fu una guerra.

All'epoca c'erano ancora i blocchi classici che facevano capo agli Stati Uniti e all'Unione Sovietica, che era ancora tale. L'offensiva politica e tecnologica di Ronald Reagan e degli Stati Uniti - allora la frontiera tecnologica era lo scudo spaziale - fu una delle ragioni, almeno secondo la storia, che misero l'Unione Sovietica non più in condizione di reggere il costo, la fatica e l'impegno tecnologico dell'azione degli Stati Uniti.

La vittoria a tavolino, che non determinò morti o vittime, di questa Terza guerra mondiale, con l'annuncio dello scudo spaziale, che avrebbe bloccato eventuali attacchi missilistici da Est, contribuì, insieme ad altre vicende, al corso della storia che poi tutti abbiamo vissuto e che oggi ha portato, pur con mille problemi nel mondo, a un diverso assetto.

Oggi c'è una guerra in corso ed è stata già descritta da molti colleghi: è la guerra delle tecnologie, con gli attacchi del *cybercrime,* che sono in corso.

Non mi voglio agganciare all'attualità, perché sinceramente l'attacco che c'è stato nel Lazio è grave ma non è il primo; voglio capire, però, perché mi ricordo che anche l'INPS qualche tempo fa se la prese con gli *hacker (Applausi)*. Voglio quindi sapere se ci sono somari veri e *hacker* finti o *hacker* veri e somari finti, perché non abbiamo ancora capito come sia finita la vicenda dell'INPS.

Ho letto oggi notizie di dipendenti che avrebbero avuto accesso a siti pornografici che contenevano virus; non lo so. Quando avremo l'Agenzia, questa riuscirà anche a distinguere la dabbenaggine tecnologica dagli attacchi, quindi non esprimo giudizi.

Siamo favorevoli all'Agenzia nazionale per la cybersicurezza, perché riteniamo che oggi la difesa delle frontiere digitali sia importante tanto quanto quella delle frontiere fisiche, quindi riteniamo che sia assolutamente necessario attrezzarsi. *(Applausi)*.

Sulle frontiere fisiche invitiamo anche il Governo a una maggiore attenzione: non vorrei che essersi concentrati sull'Agenzia per la *cybersecurity* abbia fatto un po' mollare la guardia sui confini fisici, ma questa è un'altra storia. *(Applausi)*. Riteniamo allora che sia assolutamente necessario dotarci di questo strumento.

Oggi gli interventi dei colleghi del Gruppo Forza Italia non hanno sottaciuto alcune criticità. Il senatore Mallegni diceva che anche il Dipartimento della funzione pubblica dovrebbe avere un coinvolgimento e ascoltavo la senatrice Binetti parlare della sanità. Del resto - lo dico al Governo - banche dati e attacchi sono possibili in tutti gli ambiti. L'attacco di cui si parla sta impedendo di avere il *green pass* o di prenotare i vaccini; non è stata attaccata una struttura di difesa, perché i dati sono ovunque. Oggi, a volte, esistiamo

più nella percezione digitale che non in quella fisica. Sembra un paradosso, ma è così; quindi, è assolutamente necessario agire in questa direzione.

Oggi il mondo può essere bloccato, perché, essendo connesso, basta bloccare la connessione per paralizzarlo. Ringrazio i membri del Governo presenti; forse gli impegni non hanno consentito al membro del Governo che è Autorità delegata di assistere a questo dibattito, ma sarebbe stato utile. Prima il senatore Mallegni si chiedeva che ruolo abbia il Parlamento e se qualcuno l'abbia sostituito il Parlamento. Tutti i Governi hanno molto sostituito i Parlamenti, ma non è un problema solo di questa fase.

È stata istituita l'Autorità delegata (e questo è un merito dell'attuale Governo): per Autorità delegata si intende un membro del Governo che sovraintende alle attività dei Servizi. Uno dei motivi di difficoltà del Governo precedente fu che Conte, per ragioni mai spiegate in maniera chiara in pubblico, non volle mai delegare i poteri che poi il Presidente del Consiglio in ultima istanza conserva sempre, perché è sempre tale e rimane la massima autorità di Governo. Non volle delegare quei poteri. Oggi c'è un'Autorità delegata e credo che, oltre ai Ministeri qui rappresentati (dell'attività economica, dei rapporti con il Parlamento e dell'attività produttiva), forse i Ministeri della difesa e dell'interno e tutti quelli che sono in prima linea avrebbero potuto dare un gesto di maggiore attenzione al Parlamento con la loro presenza in occasione di questo voto. *(Applausi)*. Si è fatto di corsa, come tutti abbiamo detto, e si è fatto tardi rispetto alla storia. Non ripercorro qui la cronistoria, come molti hanno fatto, sulle direttive europee, sulle sollecitazioni internazionali e sulle emergenze di ogni genere e tipo che rendono necessaria quest'Autorità, ma forse questo dibattito ci è sembrato sottovalutato e fatto in questi scorci di stagione parlamentare in cui si cerca di mettersi in paro con l'arretrato.

Ci auguriamo che quest'Autorità e questa struttura funzionino bene. Non sarà facile, perché si deve raccordare con l'attività ordinaria dei servizi di sicurezza, che restano competenti per tutte le loro funzioni, che svolgono egregiamente, con le altre autorità militari, di difesa, e con tutte le altre autorità ministeriali. Nel nucleo molti sono rappresentati e diranno la loro, ma alcuni sono assenti, quindi è un mondo complesso.

Si è anche discusso del trattamento del personale. Noi, che saremo la casta per eccellenza siamo circondati da caste. Io pure avrei preferito che, invece di dare il trattamento del personale della Banca d'Italia a questi dipendenti dell'Autorità, si togliesse ai dipendenti della Banca d'Italia il trattamento che ricevono. Invece, noi che siamo la casta e siamo circondati da caste abbiamo una motivazione: per attrarre professionalità adeguate, occorre anche un trattamento economico adeguato. Si agisce in ritardo e bisogna intervenire: servono intelligenze, come poc'anzi anche il senatore Aimi ricordava nel suo intervento; non si mette in piedi un ufficio con 300 persone scelte a caso, ma serviranno competenze, perché le attività della criminalità elettronica che devono essere fronteggiate da quest'Autorità richiedono rapidità. L'intervento distruttivo è rapido.

Una delle critiche fatte è se una struttura un po' elefantiaca, con molti raccordi, riuscirà ad agire in tempo. Non dovrà essere la sola a fare le risposte, ma le dovranno fare le strutture dei Servizi, della Difesa o anche della sanità,

come abbiamo visto. L'Autorità dovrà fecondare in tutti i vari comparti questa consapevolezza e questa necessità di difesa dei confini tecnologici, quindi guarderemo anche noi con un voto favorevole, dato con sincera predisposizione, come funzionerà questa cosa. Non sarà facile, perché si interfaccia con tanti organismi, però è un'occasione da non perdere, perché il famoso Piano nazionale di ripresa e resilienza di oltre 200 miliardi investe anche nella sicurezza tecnologica, nella modernizzazione delle reti e quindi anche nella *cybersecurity*. Dobbiamo quindi assolutamente metterci in scia, utilizzare questi fondi e rendere il Paese più sicuro, ma occorre anche attenzione.

Lo scriveva in questi giorni proprio Alessandro Sallusti in un suo editoriale, dicendo che è giusto che si faccia quest'Agenzia e che molti, preoccupati da questo Grande fratello, si distraggono di fronte al Grande fratello quotidiano che si compra la nostra vita. Basta ordinare una pizza con *delivery* e hanno tutto della nostra vita e dei nostri dati.

Non parliamo di Amazon, la nota, impunita ed esentasse Amazon, che è stata appena multata per 746 milioni *(Applausi)*, non perché non paga le tasse - lì dovrebbe versare miliardi - ma per violazioni sulla *privacy*. Non possiamo rinunciare a prenotare un cibo con il telefonino o a fare acquisti a distanza, tuttavia credo che anche qui sia un po' come la storia del *green pass* o dei vaccini: ci si preoccupa di alcune cose, ma si trascurano forme di appropriazione della nostra vita e della nostra identità che dovrebbero essere regolamentate.

Combattiamo la criminalità elettronica, ma anche l'impunità elettronica, che alcuni colossi della Rete praticano in tutto il mondo. *(Applausi)*. Votiamo quindi a favore, sperando che questa struttura ci aiuti a difendere la libertà e la sicurezza del Paese, una difesa su frontiere moderne e innovative, ma sappiamo che c'è ancora molto da fare per la nostra libertà e la nostra sicurezza. *(Applausi)*.

ARRIGONI *(L-SP-PSd'Az)*. Domando di parlare per dichiarazione di voto.

PRESIDENTE. Ne ha facoltà.

ARRIGONI *(L-SP-PSd'Az)*. Signor Presidente, colleghi, rappresentanti del Governo, di questi tempi molti Paesi sono sempre più bersaglio di attacchi *cyber*. L'Italia non ne è esente, anzi il nostro Paese è tra i più vulnerabili e dunque tra i più colpiti da minacce informatiche insidiose, sempre più numerose e diversificate, talune messe in atto da gruppi criminali, che possono chiedere un riscatto oppure vendere sul mercato le informazioni sottratte, ed altre messe in atto da attori statuali, con lo scopo di rubare informazioni sensibili, ad esempio su terapie, ricerche o brevetti.

I cyberattacchi sono in forte aumento anche a seguito della transizione digitale, del forte sviluppo e implementazione dell'intelligenza artificiale, dell'Internet of things, della tecnologia 5G e del forte aumento del traffico in Rete causato dal Covid, che ha costretto milioni di persone, lavoratori e studenti a lavorare da remoto e a studiare con la didattica a distanza (DAD), determinando un'esplosione degli attacchi informatici.

La cybersicurezza è diventata così una priorità assoluta per lo Stato, le istituzioni, le aziende e i privati, che devono assolutamente ridurre il loro grado di vulnerabilità. Ricordo quando il Copasir, da sempre attento ai temi della sicurezza *cyber* e delle sue implicazioni sulla sicurezza nazionale, con la relazione sul 5G rilasciata al Parlamento nel dicembre 2019 sottolineò i forti rischi con particolare riferimento all'impiego di apparecchiature e tecnologie cinesi nelle infrastrutture italiane. *(Applausi)*. Fu un appello che per diversi mesi è rimasto inascoltato dal Governo precedente. Non è un caso quindi che la sicurezza cibernetica costituisca uno degli interventi previsti dal Piano nazionale di ripresa e resilienza.

In coerenza con il PNRR, però con diversi anni di ritardo rispetto a Germania e Francia, che hanno già operativa da tempo una struttura consolidata che opera per difendere i rispettivi Paesi dalle minacce cibernetiche, accogliamo con favore questo decreto-legge, che definisce l'architettura nazionale di cybersicurezza e fa nascere anche in Italia un'Agenzia *cyber* nazionale, che determina un passaggio cruciale per la sicurezza nazionale nel nostro Paese. Tale razionalizzazione porta ad avere da ventitré soggetti competenti, ma dispersivi, che dialogavano su questa materia, ad un unico soggetto pubblico, che sarà l'interlocutore in Europa e nello scenario internazionale sui temi *cyber.* Sarà un'Agenzia strutturata, dotata inizialmente di trecento unità di personale, che entro il 2027 potrebbero arrivare addirittura a ottocento. Saranno figure di alta professionalità, oggetto di continua formazione, in grado di raggiungere i livelli di produzione *hardware* e *software* necessari per dotare il nostro Paese di autonomia tecnologica e renderci competitivi in campo internazionale.

Il provvedimento ci arriva blindato dalla Camera, dov'è stato oggetto di non molte modifiche, ma alcune comunque importanti che hanno visto il contributo decisivo della Lega, come quello che ha eliminato ambiguità e rischi di sovrapposizione delle competenze della nuova Agenzia con quelle delle nostre Forze di polizia, che continueranno le indagini sul *cybercrime*... *(Brusio).*

PRESIDENTE. Senatore De Siano, la invito ad abbassare il tono della voce.

ARRIGONI *(L-SP-PSd'Az)*. ...come quelle della nostra difesa, che continuerà a contrastare gli attacchi alle infrastrutture militari con la cyberdifesa e come quelle della nostra *intelligence*, il DIS e le Agenzie AISE e AISI, sulla raccolta delle informazioni.

Quello al nostro esame è un provvedimento importante, che si distingue nettamente dal pessimo e opaco progetto che il Governo Conte-*bis* lo scorso novembre stava inopportunamente proponendo nel disegno di legge di bilancio 2021 *(Applausi)* e che ipotizzava la costituzione di una fondazione sulla cybersicurezza, incardinata nel perimetro del DIS, ma con la previsione di uno statuto di cui non vi era contezza di contenuto. Con questa Agenzia vi sarà un'accelerazione del cambio di paradigma, che punta alla resilienza, alla prevenzione del rischio e della minaccia, con lo sviluppo di strumenti di *sa-*

fety, che si aggiungono agli strumenti di repressione e contenimento, cosiddetti di *security*, che vedrà da un lato sempre più investimenti sulle competenze digitali e che, dall'altro, vedrà lo Stato proteggere da attacchi informatici i sistemi pubblici, vigilando così sull'erogazione di servizi fondamentali per i cittadini.

Oggi occorre dunque accelerare sulla costituzione e sulla operatività dell'Agenzia, perché abbiamo oltre il 90 per cento dei *server* della pubblica amministrazione non in condizioni di sicurezza, per non dire che alcuni sono dei colabrodo e quindi non siamo sicuri. Inoltre, il violento, invasivo e criminoso attacco *hacker* proveniente dall'estero, forse dalla Germania, ma con probabile triangolazione, che dalla scorsa domenica notte ha colpito e infettato i *server* del CED della Regione Lazio, paralizzando anche il portale "Salute Lazio" e la rete vaccinale, bloccando le prenotazioni dei cittadini, dimostra quanto ormai sia indifferibile rendere operative le difese *cyber*, anche perché i danni sono molto gravi. La Regione è ancora in ostaggio e forse lo sarà per giorni e sulla vicenda stanno indagando i pubblici ministeri antiterrorismo. Forse è scongiurato che gli *hacker* abbiano avuto accesso alla storia sanitaria di milioni di cittadini laziali, ma comunque pare certo che i dati sono stati criptati e resi inservibili, compreso il *backup*. Purtroppo quello del Lazio non è il primo attacco che accerta la vulnerabilità del settore sanitario, che è uno dei bersagli più delicati in tempo di pandemia. Ricordo come nel marzo dello scorso anno, in pieno *lockdown*, degli *hacker* avevano preso di mira il "San Raffaele" di Milano e poi, in aprile, l'ospedale "Spallanzani" di Roma, senza contare gli attacchi non resi pubblici.

Voglio fare un'ultima considerazione, prima delle conclusioni, con riferimento al Copasir, da cui - lo rammento - io e il collega deputato Volpi, allora Presidente, ci siamo dimessi, invitando tutte le forze politiche a fare altrettanto, per ragionare sulla ricomposizione del Comitato *(Applausi)*, in modo che fosse coerente con quello che afferma la legge n.124 del 2007, nella convinzione che occorresse, allora come anche oggi, procedere necessariamente ad una attualizzazione della stessa legge disciplinante il sistema di informazione per la sicurezza della Repubblica e la nuova dottrina del segreto. Orbene, nel decreto-legge che stiamo convertendo ci sono - eccome! - modifiche dirette o indirette alla legge n. 124 del 2007, perché allarghiamo o comunque modifichiamo il perimetro delle competenze del Comitato, perché viene cambiata la modalità di azione dell'Autorità delegata, che prima aveva esclusivamente un rapporto con le Agenzie del comparto di *intelligence* o comunque con il sistema della sicurezza e, in terzo luogo, perché è cambiato anche il momento storico e tecnologico, da quando la legge è stata approvata.

Dunque la Lega ritiene che un tagliando alla legge n. 124 sia non più differibile *(Applausi)*, affinché la garanzia della presenza paritaria dei componenti del Copasir, che sarebbe opportuno diventasse proporzionale rispetto alle forze di maggioranza e minoranza di Governo, non valga solo per l'opposizione, ma anche per la stessa maggioranza, che deve in futuro potersi trovare nella condizione di poter scegliere il Presidente in votazione segreta, tra più candidati. *(Applausi)*.

Concludo confermando il voto favorevole della Lega su questo provvedimento e ovviamente augurando buon lavoro a tutti i soggetti che saranno

protagonisti nella futura istituenda Agenzia per la cybersicurezza nazionale. *(Applausi)*.

GARRUTI *(M5S)*. Domando di parlare per dichiarazione di voto.

PRESIDENTE. Ne ha facoltà.

GARRUTI *(M5S)*. Signor Presidente, nell'affrontare questo provvedimento circa le disposizioni urgenti in materia di cybersicurezza, la definizione dell'architettura nazionale di cybersicurezza e l'istituzione dell'Agenzia per la cybersicurezza nazionale non si può omettere come oggi si colmi un ritardo; al tempo stesso, il provvedimento rappresenta anche un tassello ulteriore nella più generale necessità di sviluppare in tempi brevi idonei e sempre più stringenti meccanismi di tutela cibernetica.

Per anni l'Europa ci chiedeva un interlocutore certo, definito e unitario sui temi della cybersicurezza, ma il nostro Paese si presentava con 23 soggetti competenti che interloquivano su questa materia. È stata fatta una scelta di resilienza cibernetica (dunque strutture, professionalità e formazione), necessaria a dotare il Paese di un'autonomia tecnologica che consenta di raggiungere livelli di produzione *hardware* e *software* che ci rendano competitivi nello scenario internazionale. In capo c'è un soggetto pubblico, l'Agenzia per la cybersicurezza nazionale, che dialoga con pubbliche amministrazioni e soggetti privati, con il compito non solo di definire *standard* di sicurezza applicata ai vari contesti, ma anche di coordinare eventuali sovrapposizioni con il mondo militare e dell'*intelligence*.

L'Italia non solo non può permettersi di rinunciare al progresso digitale, evitando di utilizzare tecnologie a causa di potenziali minacce introdotte, ma è anzi chiamata a usarle e gestirle al meglio, nella piena consapevolezza dei rischi, per poterne godere i benefici.

I rischi per la sicurezza informatica impattano anche sul progresso economico e sociale di un Paese. La creazione di una struttura *ad hoc*, con la direzione nelle mani dell'attore pubblico, è ormai improcrastinabile. Il provvedimento che ci accingiamo a votare è il compimento di un processo di definizione e ricomposizione di funzioni e compiti attinenti al settore della cybersicurezza, quale ambito delicato e al contempo ancora troppo vulnerabile. Nel 2019, come evidenziato nel corso delle audizioni sul decreto-legge in esame alla Camera dei deputati, sono aumentati del 246 per cento gli attacchi alle nostre infrastrutture critiche e ancor più il processo di transizione digitale e il massiccio aumento del traffico in rete dopo la prima ondata di Covid hanno costretto a milioni di persone e lavoratori del mondo, portando con sé inevitabilmente un'esplosione degli attacchi informatici.

Al centro delle recenti cronache giornalistiche c'è anche quanto accaduto nella notte tra sabato e domenica scorsi ai sistemi informatici della Regione Lazio, in particolare al centro di elaborazione dati, il sistema che gestisce l'intera infrastruttura informatica regionale. Appena ci si è accorti del problema, per evitare il proliferare dell'attacco e la possibile sottrazioni di dati, i tecnici della Regione hanno disattivato il sistema, di fatto bloccando tutti i servizi informatici regionali, il più importante dei quali in questo momento

riguarda la gestione della campagna vaccinale. Tuttavia, come inevitabilmente... *(Brusio)*.

PRESIDENTE. C'è un brusio un po' troppo forte. Lasciamo intervenire con più tranquillità il collega, grazie.

GARRUTI *(M5S)*. Grazie, signor Presidente.

Tuttavia, come inevitabile conseguenza, da domenica il sito della Regione Lazio e tutti i siti legati ai servizi informatici regionali sono irraggiungibili. La piattaforma regionale per la prenotazione degli appuntamenti delle vaccinazioni è bloccata; questo significa, in altri termini, che dal 13 agosto non sarà possibile prenotare le vaccinazioni. Se non si riattiva il servizio, al contempo è impossibile prenotare visite specialistiche, sono interrotti gli *screening* programmati, i cittadini e le imprese laziali non possono ottenere diverse autorizzazioni sanitarie ed edilizie, proprio perché sono bloccati anche tutti i servizi informatici non sanitari che di solito fanno riferimento alla Regione Lazio. Questo incidente fa perciò capire quanto la superficie di vulnerabilità sia cresciuta e quanto questa materia sia davvero importante e fondamentale. Dotare il nostro Paese di una nuova normativa che introduca contromisure volte a potenziare le nostre difese informatiche e prevenire attacchi ad infrastrutture di interesse nazionale è più che mai prioritario. Tale esigenza è infatti aumentata... *(Brusio).*

PRESIDENTE. Come dicevo prima, il collega vorrebbe che, se non desiderate ascoltarlo, almeno non lo disturbiate. Prego, senatore.

GARRUTI *(M5S)*. Grazie, Presidente. Tale esigenza è infatti aumentata negli ultimi anni, anche alla luce delle misure volte a garantire infrastrutture *cloud* sicure e centri di elaborazione dati con elevati *standard* di qualità, nella direzione di una crescente interoperabilità e condivisione delle informazioni.

Inoltre, la sicurezza cibernetica costituisce uno degli strumenti previsti dal Piano nazionale di ripresa e resilienza trasmesso dal Governo alla Commissione europea il 30 aprile 2021 e definitivamente approvato il 31 luglio 2021. In tale ambito la *cybersecurity* è uno dei sette investimenti della digitalizzazione della pubblica amministrazione, primo asse di intervento della componente 1 «Digitalizzazione, innovazione e sicurezza nella pubblica amministrazione», compresa nella missione 1 «Digitalizzazione, innovazione, competitività, cultura e turismo».

Se, da una parte, la difesa e la sicurezza nazionale e cibernetica pervadono e influenzano anche lo sviluppo economico, dall'altra parte la *privacy* di milioni di persone e la sanità, come nel caso specifico della Regione Lazio, della purtroppo non esclusa doppia estorsione (criptazione, da un lato, e sottrazione dei dati, dall'altro), devono spingerci ad approvare oggi in Assemblea un provvedimento che vada in questa direzione e che, tra l'altro, istituisce un'apposita Agenzia, che svolgerà il ruolo di Autorità nazionale per la cybersicurezza, al fine di assicurare un'azione unitaria e coordinata in tale settore,

per proseguire e completare la strada intrapresa con il cosiddetto perimetro di sicurezza cibernetica.

Per tali motivi, il MoVimento 5 Stelle voterà favorevolmente su questo provvedimento. *(Applausi)*.

PRESIDENTE. Indìco la votazione nominale con scrutinio simultaneo del disegno di legge, composto del solo articolo 1.

(Segue la votazione).

Il Senato approva. *(v. Allegato B).*

Interventi su argomenti non iscritti all'ordine del giorno

CASTELLONE *(M5S)*. Domando di parlare.

PRESIDENTE. Ne ha facoltà.

CASTELLONE *(M5S)*. Signor Presidente, ieri si sono svolti a Mantova i funerali del professor Giuseppe De Donno, ex primario di pneumologia dell'ospedale di Mantova, noto per essere stato il pioniere della terapia sperimentale anti-Covid a base della trasfusione di plasma iperimmune. Qualche mese fa, su richiesta del MoVimento 5 Stelle, avevamo invitato il professore in Commissione sanità al Senato per presentare i risultati dei suoi studi. Ricordo ancora con quale fierezza il professore, in quella sede, rivendicasse il ruolo avuto dalla sua *equipe* nella gestione della prima fase della lotta a questa pandemia.

Ricordo anche, però, il dibattito che nacque in quel periodo sulla validità o meno di questa terapia, scatenando una guerra mediatica e politica, che metteva in contrapposizione i vaccini - che, in realtà, sono strumenti di prevenzione - con le terapie, soprattutto domiciliari, che invece sono strumenti di cura.

In questi mesi la scienza, attraverso i nostri medici e i nostri ricercatori, ha dato il meglio di sé, facendo passi da gigante per comprendere questa nuova malattia e combatterla nel modo più efficace. Dall'inizio di questa pandemia ad oggi è cambiato totalmente l'approccio ai pazienti Covid: abbiamo imparato che bisogna intervenire quanto prima e le cure precoci con plasma di soggetti immuni e con anticorpi monoclonali hanno certamente rappresentato un'arma efficace. Grazie alla nostra esperienza, gli altri Paesi europei e mondiali hanno avuto più armi per curare i propri malati.

Il professor De Donno ha certamente contribuito allo sviluppo di queste conoscenze. Era un ottimo medico, stimato dai colleghi, dai suoi pazienti, una mente brillante, un uomo riservato e schietto, certamente non avvezzo al clamore mediatico che gli è stato riservato, né credo avesse mai voluto diventare argomento di scontro politico.

Al professor De Donno dico grazie per il suo contributo, per aver vissuto da vicino il dramma del Covid e anche la rinascita di chi, grazie alla sua terapia, ce la faceva. Resta nel nostro cuore la tristezza per una vita che si

spegne e l'amarezza per aver dedicato fino ad oggi poca attenzione alle terapie domiciliari.

Da parte mia, dei miei colleghi di Commissione e di tutto il mio Gruppo, esprimo profondo cordoglio e vicinanza alla sua famiglia e ai suoi colleghi. Questa morte è un dolore immenso per noi ed anche una grande sconfitta per non aver saputo proteggere e tutelare coloro che chiamiamo eroi, ma che abbiamo lasciato soli nei reparti a gestire carichi di lavoro non tollerabili e senza supporto psicologico. *(Applausi)*.

PELLEGRINI Marco *(M5S)*. Domando di parlare.

PRESIDENTE. Ne ha facoltà. Peraltro, so che interviene su un tema che avrebbe potuto riguardare l'intera Assemblea, cioè l'anniversario della strage della stazione di Bologna.

PELLEGRINI Marco *(M5S)*. Signor Presidente, come ha appunto ricordato, ieri ricorreva il quarantunesimo anniversario della strage di Bologna, in cui persero la vita 85 innocenti e oltre 200 furono i feriti. Dopo quarantuno lunghi anni si conosce solo un pezzo di verità di quella orrenda strage terroristica, che è la più grave della storia repubblicana.

Sono stati condannati in via definitiva gli esecutori materiali, individuati nei terroristi neofascisti Valerio Fioravanti, Luigi Ciavardini e Francesca Mambro, ma è in corso un ultimo processo che vede imputato Paolo Bellini, che è un soggetto che è stato ripreso da un turista sul luogo della strage pochi minuti prima. Sono stati poi condannati anche i depistatori di Stato, tra cui alcuni dirigenti infedeli del Sismi, l'allora servizio segreto militare, come il generale Musumeci e il colonnello Belmonte, oltre al faccendiere Pazienza e al gran maestro della loggia P2 Licio Gelli, che tutti insieme cercarono di proteggere gli esecutori materiali e di soffocare in tal modo la verità.

Dopo quarantuno anni, Presidente, i mandanti non sono stati ancora individuati e condannati, anche se alcuni documenti, che recentemente sono tornati magicamente alla luce, indirizzano le indagini verso Licio Gelli e Umberto Ortolani e gli ambienti della P2 che avrebbero corrisposto ingenti somme ai terroristi qualche giorno prima della strage. Queste indagini si rivolgono anche verso Federico Umberto D'Amato, che era a capo dell'Ufficio affari riservati del Ministero dell'interno, e a Mario Tedeschi, giornalista della rivista «Il Borghese».

Purtroppo sono ancora sconosciuti gli ispiratori politici di quell'attacco al cuore dello Stato e alla nostra democrazia, anche se non è difficile immaginare a quale ambito appartenessero. Valerio Fioravanti, ex baby attore, ex militante del Movimento Sociale, ex terrorista dei NAR, esecutore e/o mandante di otto omicidi, tra cui poliziotti e magistrati, esecutore - come dicevo prima - della strage di Bologna, per tutto questo ha scontato solo diciotto anni di carcere e circa otto in regime di semilibertà. Dal 2009 è libero. Durante la detenzione, anzi più esattamente durante le udienze dei vari processi in cui era imputato, ha avuto il tempo di fare un figlio con la sua compagna, anche lei terrorista, neofascista e coesecutrice della strage. Tra un omicidio e l'altro, tra una rapina e l'altra, assaltava cinema che proiettano i film

di Pier Paolo Pasolini insieme ai suoi camerati, oppure le radio private che si interessavano di politica e facevano parlare militanti sindacali o militanti femministe.

Smettere di battersi per la verità storica e processuale e pensare che ormai è passato troppo tempo per accettarla sarebbe fare un favore ai fascisti come Fioravanti, Mambro, Ciavardini e ai loro mandanti e darla vinta a chi voleva uccidere, nel terrore, la nostra democrazia e la nostra libertà.

Non dobbiamo permetterlo, né dimenticare il sangue versato da cittadini inermi e innocenti. *(Applausi)*.

GASPARRI *(FIBP-UDC)*. Domando di parlare.

PRESIDENTE. Ne ha facoltà.

GASPARRI *(FIBP-UDC)*. Signor Presidente, nel ricordare, a quarantuno anni da quel tragico evento, le vittime e i feriti della strage di Bologna, voglio cogliere l'occasione di questo intervento per dire che ho apprezzato l'annuncio che proprio ieri, a Bologna, ha dato il ministro della giustizia Cartabia, dicendo che alcuni documenti riguardanti vicende della P2 e altri accadimenti di quegli anni saranno desecretati. Voglio però dire in quest'Aula, una volta di più, che noi attendiamo che venga rispettato un deliberato assunto all'unanimità nella scorsa legislatura dalla Commissione d'inchiesta sul caso Moro, di cui facevo parte insieme al senatore Giovanardi e altri colleghi. Chiedemmo la desecretazione di una serie di documenti che abbiamo letto nei vincoli di riservatezza che la Commissione di inchiesta ha e che sono attinenti a quella drammatica estate del 1980.

Conosciamo la verità giudiziaria. Le vicende di quella tragica estate videro prima la vicenda di Ustica, mai realmente chiarita fino in fondo, e poi la vicenda di Bologna, per la quale c'è una verità giudiziaria accertata. Tuttavia, i documenti che noi abbiamo visto e che il presidente del Consiglio dell'epoca, Paolo Gentiloni, ci assicurò sarebbero stati desecretati e non sono ricompresi in quelli di cui ha parlato ieri il ministro Cartabia, sono importanti.

Ieri il presidente della Camera dei deputati, Roberto Fico, ha parlato di una mistificazione su queste vicende. Sì, c'è una mistificazione, ma a mio avviso la si scopre guardando quelle carte. Il giornalista Grignetti, su «La Stampa» le ha pubblicate anni fa, quindi è il segreto di Pulcinella. I rapporti che venivano dal Medio Oriente in quegli anni fanno capire chiaramente la matrice della vicenda di Ustica e della strage di Bologna. Quei documenti smentiscono in maniera totale le verità giudiziarie accertate, sulle quali si costruiscono leggende che anche prima ho sentito riecheggiare in quest'Aula.

Insisto affinché vengano desecretati quegli atti e i famosi rapporti del colonnello Giovannone dal Libano, che dicono chi ha fatto Ustica e chi la strage di Bologna, smentendo sentenze basate su fatti non reali. Infatti, i fatti reali e quei rapporti riservati dicono un'altra verità, che però qualcuno non vuole ascoltare per continuare a fare le leggende, come abbiamo sentito anche questa sera in questa sede. *(Applausi)*.

PRESIDENTE. Le leggerà anche il senatore Pellegrini.

Atti e documenti, annunzio

PRESIDENTE. Le mozioni, le interpellanze e le interrogazioni pervenute alla Presidenza, nonché gli atti e i documenti trasmessi alle Commissioni permanenti ai sensi dell'articolo 34, comma 1, secondo periodo, del Regolamento sono pubblicati nell'allegato B al Resoconto della seduta odierna.

Ordine del giorno per la seduta di mercoledì 4 agosto 2021

PRESIDENTE. Il Senato tornerà a riunirsi in seduta pubblica domani, mercoledì 4 agosto, alle ore 11, con il seguente ordine del giorno:

I. Discussione congiunta dei disegni di legge:

Rendiconto generale dell'Amministrazione dello Stato per l'esercizio finanziario 2020 *(voto finale con la presenza del numero legale) - Relatore* PESCO *(Relazione orale)* (2308)

- Disposizioni per l'assestamento del bilancio dello Stato per l'anno finanziario 2021 *(voto finale con la presenza del numero legale) - Relatrice* FAGGI Antonella *(Relazione orale)* (2309)

II. Comunicazioni del Presidente, ai sensi dell'articolo 126-*bis*, comma 2-*bis*, del Regolamento, sul ddl. n. 2318 - Delega al Governo in materia di spettacolo *(collegato alla manovra di finanza pubblica)*

III. Discussione dei documenti:

1. Risoluzione approvata dalle Commissioni 3ª e 4ª riunite, ai sensi dell'articolo 50, comma 2, del Regolamento, a conclusione dell'esame dell'affare assegnato sulla relazione analitica sulle missioni internazionali in corso e sullo stato degli interventi di cooperazione allo sviluppo a sostegno dei processi di pace e di stabilizzazione, riferita all'anno 2020, anche al fine della relativa proroga per l'anno 2021, deliberata dal Consiglio dei ministri il 17 giugno 2021 (*Doc*. XXIV, n. 48)
2. Risoluzione adottata dalle Commissioni 3ª e 4ª riunite, ai sensi dell'articolo 50, comma 2, del Regolamento, a conclusione dell'esame dell'affare assegnato sulla deliberazione del Consiglio dei ministri in merito alla prosecuzione delle missioni internazionali in corso e alla partecipazione dell'Italia a ulteriori missioni internazionali per l'anno 2021, adottata il 17 giugno 2021 (*Doc*. XXIV, n. 49)

La seduta è tolta *(ore 19,28)*.

Allegato A

DISEGNO DI LEGGE

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**)**

ARTICOLO 1 DEL DISEGNO DI LEGGE DI CONVERSIONE E ALLEGATO RECANTE LE MODIFICAZIONI APPORTATE AL DECRETO-LEGGE, NEL TESTO APPROVATO DALLA CAMERA DEI DEPUTATI

Art. 1.

1. Il 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, è convertito in legge con le modificazioni riportate in allegato alla presente legge.

2. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale*.

N.B. Approvato il disegno di legge composto del solo articolo 1.

Allegato

MODIFICAZIONI APPORTATE IN SEDE DI CONVERSIONE AL DECRETO-LEGGE 14 GIUGNO 2021, N. 82

All'articolo 1:

il comma 1 è sostituito dal seguente:

« 1. Ai fini del presente decreto si intende per:

a) cybersicurezza, l'insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico;

b) resilienza nazionale nello spazio cibernetico, le attività volte a prevenire un pregiudizio per la sicurezza nazionale come definito dall'articolo 1, comma

1, lettera *f)*, del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131;

c) decreto-legge perimetro, il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica;

d) decreto legislativo NIS, il decreto legislativo 18 maggio 2018, n. 65, di attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione;

e) strategia nazionale di cybersicurezza, la strategia di cui all'articolo 6 del decreto legislativo NIS ».

All'articolo 2:

al comma 1:

alla lettera a)*, le parole:* « , anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico » *sono soppresse*;

alla lettera c) *sono aggiunte, in fine, le seguenti parole:* « , previa deliberazione del Consiglio dei ministri »;

al comma 2, la parola: « lett. » *è sostituita dalla seguente:* « lettera »;

al comma 3, le parole: « il presidente del COPASIR » *sono sostituite dalle seguenti:* « il Comitato parlamentare per la sicurezza della Repubblica (COPASIR), di cui all'articolo 30 della legge 3 agosto 2007, n. 124, e le Commissioni parlamentari competenti » *e sono aggiunte, in fine, le seguenti parole:* « , del presente articolo ».

All'articolo 3:

al comma 1, le parole: « alla medesima Autorità » *sono sostituite dalle seguenti:* « all'Autorità » *e le parole:* « legge n. 124 del 2007, ove istituita, » *sono sostituite dalle seguenti:* « legge 3 agosto 2007, n. 124, ove istituita, denominata di seguito: "Autorità delegata", ».

All'articolo 4:

al comma 1, le parole: « , anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico » *sono soppresse*;

al comma 4, dopo le parole: « dell'Agenzia » *sono inserite le seguenti:* « per la cybersicurezza nazionale »;

al comma 5, *le parole:* « il direttore generale del DIS, il direttore dell'AISE, il direttore dell'AISI, » *sono soppresse;*

al comma 6, la parola: « CISR » *è sostituita dalle seguenti:* « Comitato interministeriale per la sicurezza della Repubblica (CISR), di cui all'articolo 5 della legge 3 agosto 2007, n. 124, ».

All'articolo 5:

al comma 1, le parole: « , anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico *» sono soppresse*;

al comma 3, al primo periodo, le parole: « legge n. 400 del 1988 » *sono sostituite dalle seguenti:* « legge 23 agosto 1988, n. 400 » *e, al terzo periodo, la parola:* « Direttore » *è sostituita dalla seguente:* « direttore » *e la parola:* « vicedirettore » *è sostituita dalle seguenti:* « vice direttore »;

al comma 5, *dopo le parole:* « di altre amministrazioni, » *sono inserite le seguenti: «* delle Forze armate, *»*;

al comma 6, *dopo le parole:* « il COPASIR » *sono inserite le seguenti: « ,* ai sensi di quanto previsto dall'articolo 31, comma 3, della legge 3 agosto 2007, n. 124, *».*

All'articolo 6:

al comma 1, le parole: « nell'ambito delle risorse disponibili *» sono sostituite dalle seguenti: «* nell'ambito delle risorse finanziarie destinate all'Agenzia ai sensi dell'articolo 18, comma 1 »;

al comma 3, *dopo le parole:* « previo parere » *sono inserite le seguenti: «* delle Commissioni parlamentari competenti per materia e per i profili finanziari e, per i profili di competenza, *».*

All'articolo 7:

al comma 1:

alla lettera e):

al numero 1), le parole: « comma 1 » *sono sostituite dalle seguenti:* « paragrafo 1 »;

al numero 2), le parole: « comma 6 » *sono sostituite dalle seguenti:* « paragrafo 6 » *e le parole:* « punto 1) » *sono sostituite dalle seguenti:* « numero 1) della presente lettera »;

alla lettera i)*, la parola: «* DIS *» è sostituita dalle seguenti: «* Dipartimento delle informazioni per la sicurezza (DIS), di cui all'articolo 4 della legge 3 agosto 2007, n. 124, »;

alla lettera m)*, le parole:* « nonché in materia » *sono sostituite dalle seguenti:* « nonché quelle in materia »;

dopo la lettera m) *sono inserite le seguenti:*

« m-bis) assume le iniziative idonee a valorizzare la crittografia come strumento di cybersicurezza, anche attraverso un'apposita sezione dedicata nell'ambito della strategia di cui alla lettera *b)*. 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;

m-ter) provvede alla qualificazione dei servizi *cloud* per la pubblica amministrazione nel rispetto della disciplina dell'Unione europea e del regolamento

di cui all'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221 »;

alla lettera n) *sono aggiunte, in fine, le seguenti parole:* « . A tale fine, promuove iniziative di partenariato pubblico-privato per rendere effettive tali capacità »;

alla lettera q)*, le parole:* « istituzioni, ed enti » *sono sostituite dalle seguenti:* « istituzioni ed enti »;

alla lettera r) *sono aggiunte, in fine, le seguenti parole: «* e, in particolare, con il Ministero della difesa per gli aspetti inerenti alla ricerca militare. L'Agenzia può altresì promuovere la costituzione di aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione e il reclutamento di personale nei settori avanzati dello sviluppo della cybersicurezza, nonché promuovere la realizzazione di studi di fattibilità e di analisi valutative finalizzati a tale scopo *»*;

alla lettera s)*, le parole:* « Ministero degli esteri » *sono sostituite dalle seguenti:* « Ministero degli affari esteri »;

alla lettera t)*, le parole:* « Ministero degli esteri » *sono sostituite dalle seguenti:* « Ministero degli affari esteri » *e sono aggiunte, in fine, le seguenti parole:* « e, in particolare, con il Ministero della difesa per gli aspetti inerenti a progetti e iniziative in collaborazione con la NATO e con l'Agenzia europea per la difesa »;

alla lettera v), *dopo le parole:* « nel campo della cybersicurezza, » *sono inserite le seguenti: «* in particolare favorendo l'attivazione di percorsi formativi universitari in materia, *» e sono aggiunte, in fine, le seguenti parole:* « ; nello svolgimento di tali compiti, l'Agenzia può avvalersi anche delle strutture formative e delle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri interessati »;

dopo la lettera v) *è inserita la seguente:*

« v-bis) può predisporre attività di formazione specifica riservate ai giovani che aderiscono al servizio civile regolate sulla base di apposite convenzioni. In ogni caso, il servizio prestato è, a tutti gli effetti, riconosciuto come servizio civile *»*;

dopo il comma 1 è inserito il seguente:

« 1-*bis*. Anche ai fini dell'esercizio delle funzioni di cui al comma 1, lettere *r), s), t), u), v), z)* e *aa),* presso l'Agenzia è istituito, con funzioni di consulenza e di proposta, un Comitato tecnico-scientifico, presieduto dal direttore generale della medesima Agenzia, o da un dirigente da lui delegato, e composto da personale della stessa Agenzia e da qualificati rappresentanti dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza, designati con decreto del Presidente del Consiglio dei ministri. La com-

posizione e l'organizzazione del Comitato tecnico-scientifico sono disciplinate secondo le modalità e i criteri definiti dal regolamento di cui all'articolo 6, comma 1. Per la partecipazione al Comitato tecnico-scientifico non sono previsti gettoni di presenza, compensi o rimborsi di spese ».

All'articolo 8:

al comma 2, primo periodo, le parole: « o dal vice direttore generale da lui designato *» sono sostituite dalle seguenti: «* o, per sua delega, dal vice direttore generale *» e le parole:* « dell'AISE, dell'AISI, di ciascuno dei Ministeri rappresentati nel Comitato di cui all'articolo 5 della legge n. 124 del 2007, del Ministero dell'università e della ricerca, del Ministro delegato per l'innovazione tecnologica e la transizione digitale » *sono sostituite dalle seguenti:* « dell'Agenzia informazioni e sicurezza esterna (AISE), di cui all'articolo 6 della legge 3 agosto 2007, n. 124, dell'Agenzia informazioni e sicurezza interna (AISI), di cui all'articolo 7 della legge n. 124 del 2007, di ciascuno dei Ministeri rappresentati nel CIC »;

al comma 3, primo periodo, dopo le parole: « I componenti » *sono inserite le seguenti:* « del Nucleo »;

dopo il comma 4 è inserito il seguente:

« 4-*bis*. Ai componenti del Nucleo non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati *».*

All'articolo 9:

al comma 1:

alla lettera b)*, le parole:* « decreto-legge n. 174 del 2015, convertito, con modificazioni, dalla legge n. 198 del 2015 » *sono sostituite dalle seguenti:* « decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198 »;

alla lettera c)*, le parole:* « in esercitazioni » *sono sostituite dalle seguenti:* « a esercitazioni »;

alla lettera e)*, le parole:* « riceve, per il tramite del CSIRT Italia, le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi, dal DIS, dall'AISE e dall'AISI » *sono sostituite dalle seguenti:* « acquisisce, anche per il tramite del CSIRT Italia, le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi dagli organismi di informazione di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124 » *e le parole:* « decreto-legge n. 144 del 2005, convertito, con modificazioni, dalla legge n. 155 del 2005 » *sono sostituite dalle seguenti:* « decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 ».

All'articolo 10:

il comma 2 è soppresso;

al comma 3, primo periodo, le parole: « , del Ministero delle infrastrutture e della mobilità sostenibili, » *sono sostituite dalla seguente:* « e »;

al comma 4, le parole: « di natura cibernetica, » *sono sostituite dalle seguenti:* « di natura cibernetica »;

al comma 5:

all'alinea, le parole: « decreto-legge n. 174 del 2015, convertito, con modificazioni, dalla legge n. 198 del 2015 » *sono sostituite dalle seguenti:* « decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198 »;

alla lettera e)*, le parole:* « dell'UE » *sono sostituite dalle seguenti:* « dell'Unione europea ».

All'articolo 11:

al comma 1, le parole: « Con legge di bilancio » *sono sostituite dalle seguenti:* « Con la legge di bilancio »;

al comma 2, lettera e)*, la parola:* « contribuiti » *è sostituita dalla seguente:* « contributi »;

al comma 3:

alla lettera a)*, dopo le parole:* « del CIC » *è inserito il seguente segno d'interpunzione:* « , »;

alla lettera b)*, le parole:* « sono trasmessi, al » *sono sostituite dalle seguenti:* « sono trasmessi alle Commissioni parlamentari competenti e al »;

al comma 4, le parole: « e per quelle svolte in raccordo con il Sistema di informazione per la sicurezza della Repubblica di cui alla legge n. 124 del 2007 » *sono soppresse.*

All'articolo 12:

al comma 1:

al primo periodo, le parole: « di tutela della sicurezza nazionale nello spazio cibernetico attribuite all'Agenzia e tenuto conto delle attività svolte dalla stessa in raccordo con il Sistema di informazione per la sicurezza della Repubblica di cui alla legge n. 124 del 2007 *» sono sostituite dalle seguenti:* « volte alla tutela della sicurezza nazionale nello spazio cibernetico attribuite all'Agenzia »;

al secondo periodo, dopo le parole: « per il personale dell'Agenzia » *sono inserite le seguenti*: « di cui al comma 2, lettera *a)*, »;

al terzo periodo, le parole: « sia con riferimento » *sono sostituite dalle seguenti:* « con riferimento sia » *e dopo le parole:* « in servizio che » *sono inserite le seguenti:* « al trattamento »;

al comma 2:

all'alinea, le parole: « nei limiti delle risorse finanziarie disponibili » *sono sostituite dalle seguenti:* « nell'ambito delle risorse finanziarie destinate all'Agenzia ai sensi dell'articolo 18, comma 1 »;

alla lettera c)*, dopo le parole:* « composto da personale » *è inserito il seguente segno d'interpunzione:* « , » *e le parole:* « analoga posizione, prevista » *sono sostituite dalle seguenti:* « analoga posizione prevista »;

al comma 5, le parole: « al presidente del » *sono sostituite dalle seguenti:* « alle Commissioni parlamentari competenti e al »;

al comma 7, le parole: « Fatto salvo quanto previsto dall'articolo 42 della legge n. 124 del 2007, » *sono soppresse*;

al comma 8, dopo le parole: « previo parere » *sono inserite le seguenti:* « delle Commissioni parlamentari competenti per materia e per i profili finanziari e, per i profili di competenza, ».

All'articolo 14:

al comma 2, le parole: « in raccordo con il Sistema di informazione per la sicurezza della Repubblica di cui alla legge n. 124 del 2007, nonché in relazione agli ambiti di attività dell'Agenzia sottoposti al controllo del Comitato ai sensi del presente decreto » *sono sostituite dalle seguenti: «* negli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico relativamente ai profili di competenza del Comitato ».

All'articolo 15:

al comma 1:

alla lettera e)*, capoverso comma 6, lettera* b)*, dopo le parole: «* sono valutate » *sono inserite le seguenti: «* ed eventualmente integrate, d'intesa con le autorità di settore, »;

alla lettera f)*, le parole:* « dalle seguenti: "cybersicurezza" »*, ovunque ricorrono, sono sostituite dalle seguenti:* « dalla seguente: "cybersicurezza" »;

alla lettera g)*, capoverso Art. 7:*

al comma 1, lettera d)*, le parole:* « delle Regioni » *sono sostituite dalle seguenti:* « dalle Regioni »;

al comma 8, alinea, dopo le parole: « dal presente articolo » *è inserito il seguente segno d'interpunzione:* « , » *e le parole:* « a decorrere dal » *sono sostituite dalle seguenti:* « annui a decorrere dall'anno »;

alla lettera h)*, le parole:* « l'Agenzia di cybersicurezza » *sono sostituite dalle seguenti:* « l'Agenzia per la cybersicurezza »;

alla lettera i)*, capoverso 1, al secondo periodo, le parole:* « nazionale, un » *sono sostituite dalle seguenti:* « nazionale un » *e, al quinto periodo, dopo le parole:* « o rimborsi » *è inserita la seguente:* « di »;

al comma 2:

alla lettera a) *sono aggiunte, in fine, le seguenti parole:* « , come sostituito dal comma 1, lettera *g)*, del presente articolo »;

alla lettera c) *sono aggiunte, in fine, le seguenti parole:* « , come modificato dalla lettera *d)* del presente comma ».

All'articolo 16:

al comma 1, le parole: « legge n. 124 del 2007 » *sono sostituite dalle seguenti:* « legge 3 agosto 2007, n. 124 »;

al comma 2, dopo le parole: « è abrogato » *sono aggiunte le seguenti:* « a decorrere dal 1° gennaio 2023 »;

al comma 5, dopo le parole: « cybersicurezza nazionale » *sono inserite le seguenti: «* , fatta eccezione per le disposizioni dell'articolo 1, commi 2, lettera *b)*, e 2-*ter*, del medesimo decreto-legge perimetro, »;

al comma 8, le parole: « di cui agli articoli 3 del decreto del Presidente del Consiglio dei ministri n. 131 del 2020 » *sono sostituite dalle seguenti:* « di cui all'articolo 3 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131 »;

al comma 9:

dopo la lettera a) *sono inserite le seguenti:*

« a-bis) all'articolo 1, comma 7, lettera *c)*, le parole: "dell'organismo tecnico di supporto al CISR" sono sostituite dalle seguenti: "del Tavolo interministeriale di cui all'articolo 6 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131";

a-ter) all'articolo 1, comma 2, la lettera *b)* è sostituita dalla seguente:

"*b)* sono definiti, sulla base di un'analisi del rischio e di un criterio di gradualità che tenga conto delle specificità dei diversi settori di attività, i criteri con i quali i soggetti di cui al comma 2-*bis* predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, fermo restando che, per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate, si applica quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge 3 agosto 2007, n. 124; all'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, il Tavolo interministeriale di cui all'articolo 6 del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; entro sei mesi dalla data della comunicazione, prevista dal comma 2-*bis*, a ciascuno dei soggetti iscritti nell'elenco di cui al medesimo comma, i soggetti pubblici e quelli di cui all'articolo 29 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, nonché quelli privati, di cui al citato comma 2-*bis*, trasmettono tali elenchi all'Agenzia per la cybersicurezza nazionale, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la cybersicurezza; il Dipartimento delle informazioni per la sicurezza, l'Agenzia informazioni e sicurezza esterna

(AISE) e l'Agenzia informazioni e sicurezza interna (AISI) ai fini dell'esercizio delle funzioni istituzionali previste dagli articoli 1, comma 3-*bis*, 4, 6 e 7 della legge n. 124 del 2007, nonché l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155*,* accedono a tali elenchi per il tramite della piattaforma digitale di cui all'articolo 9, comma 1, del regolamento di cui al decreto del Presidente del Consiglio dei ministri n. 131 del 2020, costituita presso l'Agenzia per la cybersicurezza nazionale";

a-quater) all'articolo 1, dopo il comma 2-*bis* è inserito il seguente:

"*2-ter*. Gli elenchi dei soggetti di cui alla lettera *a)* del comma 2 del presente articolo sono trasmessi al Dipartimento delle informazioni per la sicurezza, che provvede anche a favore dell'AISE e dell'AISI ai fini dell'esercizio delle funzioni istituzionali previste dagli articoli 1, comma 3-*bis*, 4, 6 e 7 della legge 3 agosto 2007, n. 124" »;

alla lettera c)*, numero 1), capoverso 1, secondo periodo, le parole:* « di predetti » *sono sostituite dalle seguenti:* « dei predetti »;

al comma 10, capoverso 3-bis*, decimo periodo, dopo le parole:* « sanzione amministrativa pecuniaria » *sono inserite le seguenti:* « del pagamento di una somma »;

al comma 11, le parole: « 135 del decreto legislativo » *sono sostituite dalle seguenti:* « 135, comma 1, del codice del processo amministrativo, di cui all'allegato 1 al decreto legislativo » *e sono aggiunte, in fine, le seguenti parole:* « e alla lettera *o*) le parole: "e dell'AISE" sono sostituite dalle seguenti: ", dell'AISE e dell'Agenzia per la cybersicurezza nazionale" »;

al comma 13 sono aggiunte, in fine, le seguenti parole: « e sono aggiunte, in fine, le seguenti parole: "nonché le modalità del procedimento di qualificazione dei servizi *cloud* per la pubblica amministrazione" ».

All'articolo 17:

al comma 5, lettera b)*, dopo le parole:* « amministrazioni interessate, » *sono inserite le seguenti:* « nel rispetto delle specifiche norme riguardanti l'organizzazione e il funzionamento, »;

dopo il comma 5 è inserito il seguente:

« 5-*bis*. Fino alla scadenza dei termini indicati nel decreto o nei decreti di cui al comma 5, lettera *b)*, la gestione delle risorse finanziarie relative alle funzioni trasferite, compresa la gestione dei residui passivi e perenti, è esercitata dalle amministrazioni cedenti. A decorrere dalla medesima data sono trasferiti in capo all'Agenzia i rapporti giuridici attivi e passivi relativi alle funzioni trasferite »;

al comma 6, le parole: « di AgID » *sono sostituite dalle seguenti:* « dell'AgID. Nelle more dell'adozione dei decreti di cui al comma 5, il regolamento di cui all'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179,

convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, è adottato dall'AgID, d'intesa con la competente struttura della Presidenza del Consiglio dei ministri »;

al comma 7:

il primo periodo è sostituito dai seguenti: « Al fine di assicurare la prima operatività dell'Agenzia, il direttore generale dell'Agenzia, fino all'adozione dei regolamenti di cui all'articolo 11, commi 3 e 4, identifica, assume e liquida gli impegni di spesa che verranno pagati a cura del DIS, nell'ambito delle risorse destinate all'Agenzia. A tale fine è istituito un apposito capitolo nel bilancio del DIS »;

al secondo periodo, le parole: « commi 3 e 5, delle spese effettuate ai sensi del presente comma, il Presidente del Consiglio dei ministri ne dà informazione al COPASIR » *sono sostituite dalle seguenti:* « commi 3 e 4, il Presidente del Consiglio dei ministri dà informazione al COPASIR delle spese effettuate ai sensi del presente comma »;

il comma 8 è sostituito dai seguenti:

« 8. Al fine di assicurare la prima operatività dell'Agenzia, dalla data della nomina del direttore generale dell'Agenzia e nel limite del 30 per cento della dotazione organica complessiva iniziale di cui all'articolo 12, comma 4:

a) il DIS mette a disposizione il personale impiegato nell'ambito delle attività relative allo svolgimento delle funzioni oggetto di trasferimento, con modalità da definire mediante intese con lo stesso Dipartimento;

b) l'Agenzia si avvale, altresì, di unità di personale appartenenti al Ministero dello sviluppo economico, all'Agenzia per l'Italia digitale, ad altre pubbliche amministrazioni e ad autorità indipendenti, per un periodo massimo di sei mesi, prorogabile una sola volta per un massimo di ulteriori sei mesi, messo a disposizione dell'Agenzia stessa su specifica richiesta e secondo modalità individuate mediante intese con le rispettive amministrazioni di appartenenza.

8-*bis*. Gli oneri derivanti dall'attuazione del comma 8 restano a carico dell'amministrazione di appartenenza »;

al comma 9:

al primo periodo, dopo le parole: « di cui al comma 8 » *sono inserite le seguenti:* « del presente articolo »;

dopo il primo periodo è inserito il seguente: « Il personale di cui al comma 8, lettera *a)*, è inquadrato, a decorrere dal 1° gennaio 2022, nel ruolo di cui all'articolo 12, comma 2, lettera *a)*, secondo le modalità definite dal regolamento di cui all'articolo 12, comma 1 »;

al secondo periodo, dopo le parole: « al comma 8, » *sono inserite le seguenti:* « lettera *b)*, »;

dopo il comma 10 sono aggiunti i seguenti:

« 10-*bis*. In sede di prima applicazione del presente decreto:

a) la prima relazione di cui all'articolo 14, comma 1, è trasmessa entro il 30 novembre 2022;

b) entro il 31 ottobre 2022, il Presidente del Consiglio dei ministri trasmette alle Camere una relazione che dà conto dello stato di attuazione, al 30 settembre 2022, delle disposizioni di cui al presente decreto, anche al fine di formulare eventuali proposte in materia.

10-*ter*. I pareri delle Commissioni parlamentari competenti per materia e per i profili finanziari e del COPASIR previsti dal presente decreto sono resi entro il termine di trenta giorni dalla trasmissione dei relativi schemi di decreto, decorso il quale il Presidente del Consiglio dei ministri può comunque procedere all'adozione dei relativi provvedimenti ».

All'articolo 18:

al comma 2, la parola: « corrispondete » *è sostituita dalla seguente:* « corrispondente » *e le parole:* « dell'autorizzazione di spesa » *sono sostituite dalle seguenti:* « del Fondo »;

al comma 3, le parole: « dall'entrata in servizio » *sono sostituite dalle seguenti:* « dall'inizio del funzionamento » *e le parole:* « in spesa » *sono sostituite dalle seguenti:* « alla spesa »;

al comma 4 sono aggiunte, in fine, le seguenti parole: « del presente articolo »;

al comma 5, le parole: « per l'attuazione del presente decreto » *sono soppresse.*

ARTICOLI DA 1 A 4 DEL DECRETO-LEGGE NEL TESTO COMPRENDENTE LE MODIFICAZIONI APPORTATE DALLA CAMERA DEI DEPUTATI

Articolo 1.

(Definizioni)

1. Ai fini del presente decreto si intende per:

a) cybersicurezza, l'insieme delle attività, ferme restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico;

b) resilienza nazionale nello spazio cibernetico, le attività volte a prevenire un pregiudizio per la sicurezza nazionale come definito dall'articolo 1, comma 1, lettera *f)*, del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131;

c) decreto-legge perimetro, il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica;

d) decreto legislativo NIS, il decreto legislativo 18 maggio 2018, n. 65, di attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione;

e) strategia nazionale di cybersicurezza, la strategia di cui all'articolo 6 del decreto legislativo NIS.

Articolo 2.

(Competenze del Presidente del Consiglio dei ministri)

1. Al Presidente del Consiglio dei ministri sono attribuite in via esclusiva:

a) l'alta direzione e la responsabilità generale delle politiche di cybersicurezza;

b) l'adozione della strategia nazionale di cybersicurezza, sentito il Comitato interministeriale per la cybersicurezza (CIC) di cui all'articolo 4;

c) la nomina e la revoca del direttore generale e del vice direttore generale dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 5, previa deliberazione del Consiglio dei ministri.

2. Ai fini dell'esercizio delle competenze di cui al comma 1, lettera *a),* e dell'attuazione della strategia nazionale di cybersicurezza, il Presidente del Consiglio dei ministri, sentito il CIC, impartisce le direttive per la cybersicurezza ed emana ogni disposizione necessaria per l'organizzazione e il funzionamento dell'Agenzia per la cybersicurezza nazionale.

3. Il Presidente del Consiglio dei ministri informa preventivamente il Comitato parlamentare per la sicurezza della Repubblica (COPASIR), di cui all'articolo 30 della legge 3 agosto 2007, n. 124, e le Commissioni parlamentari competenti circa le nomine di cui al comma 1, lettera *c)*, del presente articolo.

Articolo 3.

(Autorità delegata)

1. Il Presidente del Consiglio dei ministri, ove lo ritenga opportuno, può delegare all'Autorità di cui all'articolo 3 della legge 3 agosto 2007, n. 124, ove istituita, denominata di seguito: « Autorità delegata », le funzioni di cui al presente decreto che non sono ad esso attribuite in via esclusiva.

2. Il Presidente del Consiglio dei ministri è costantemente informato dall'Autorità delegata sulle modalità di esercizio delle funzioni delegate ai sensi del presente decreto e, fermo restando il potere di direttiva, può in qualsiasi momento avocare l'esercizio di tutte o di alcune di esse.

3. L'Autorità delegata, in relazione alle funzioni delegate ai sensi del presente decreto, partecipa alle riunioni del Comitato interministeriale per la transizione digitale di cui all'articolo 8 del decreto-legge 1° marzo 2021, n. 22, convertito, con modificazioni, dalla legge 22 aprile 2021, n. 55.

Articolo 4.

(Comitato interministeriale per la cybersicurezza)

1. Presso la Presidenza del Consiglio dei ministri è istituito il Comitato interministeriale per la cybersicurezza (CIC), con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza.

2. Il Comitato:

a) propone al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale;

b) esercita l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza;

c) promuove l'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, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza;

d) esprime il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la cybersicurezza nazionale.

3. Il Comitato è presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri e della cooperazione internazionale, dal Ministro dell'interno, dal Ministro della giustizia, dal Ministro della difesa, dal Ministro dell'economia e delle finanze, dal Ministro dello sviluppo economico, dal Ministro della transizione ecologica, dal Ministro dell'università e della ricerca, dal Ministro delegato per l'innovazione tecnologica e la transizione digitale e dal Ministro delle infrastrutture e della mobilità sostenibili.

4. Il direttore generale dell'Agenzia per la cybersicurezza nazionale svolge le funzioni di segretario del Comitato.

5. Il Presidente del Consiglio dei ministri può chiamare a partecipare alle sedute del Comitato, anche a seguito di loro richiesta, senza diritto di voto, altri componenti del Consiglio dei ministri, nonché altre autorità civili e militari di cui, di volta in volta, ritenga necessaria la presenza in relazione alle questioni da trattare.

6. Il Comitato svolge altresì le funzioni già attribuite al Comitato interministeriale per la sicurezza della Repubblica (CISR), di cui all'articolo 5 della legge 3 agosto 2007, n. 124, dal decreto-legge perimetro e dai relativi provvedimenti attuativi, fatta eccezione per quelle previste dall'articolo 5 del medesimo decreto-legge perimetro.

ORDINI DEL GIORNO

G4.100

RAUTI, MALAN

Non posto in votazione (*)

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.

(*) Accolto dal Governo

G4.101

RAUTI, MALAN

V. testo 2

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.

G4.101 (testo 2)

RAUTI, MALAN

Non posto in votazione (*)

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,

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.

(*) Accolto dal Governo

G4.102

MALLEGNI

Ritirato

Il Senato,

in sede di discussione 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;

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

Ritirato

Il Senato,

in sede di discussione 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;

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

Ritirato

Il Senato,

in sede di discussione 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;

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

Ritirato

Il Senato,

in sede di discussione 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;

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.

ARTICOLO 5 DEL DECRETO-LEGGE NEL TESTO COMPRENDENTE LE MODIFICAZIONI APPORTATE DALLA CAMERA DEI DEPUTATI

Articolo 5.

(Agenzia per la cybersicurezza nazionale)

1. È istituita, a tutela degli interessi nazionali nel campo della cybersicurezza, l'Agenzia per la cybersicurezza nazionale, denominata ai fini del presente decreto « Agenzia », con sede in Roma.

2. 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 presente decreto. Il Presidente del Consiglio dei ministri e l'Autorità delegata, ove istituita, si avvalgono dell'Agenzia per l'esercizio delle competenze di cui al presente decreto.

3. Il direttore generale dell'Agenzia è nominato tra soggetti appartenenti a una delle categorie di cui all'articolo 18, comma 2, della legge 23 agosto 1988, n. 400, in possesso di una documentata esperienza di elevato livello nella gestione di processi di innovazione. Gli incarichi del direttore generale e del

vice direttore generale hanno la durata massima di quattro anni e sono rinnovabili, con successivi provvedimenti, per una durata complessiva massima di ulteriori quattro anni. Il direttore generale ed il vice direttore generale, ove provenienti da pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, sono collocati fuori ruolo o in posizione di comando o altra analoga posizione, secondo gli ordinamenti di appartenenza. Per quanto previsto dal presente decreto, il direttore generale dell'Agenzia è il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata, ove istituita, ed è gerarchicamente e funzionalmente sovraordinato al personale dell'Agenzia. Il direttore generale ha la rappresentanza legale dell'Agenzia.

4. L'attività dell'Agenzia è regolata dal presente decreto e dalle disposizioni la cui adozione è prevista dallo stesso.

5. L'Agenzia può richiedere, anche sulla base di apposite convenzioni e nel rispetto degli ambiti di precipua competenza, la collaborazione di altri organi dello Stato, di altre amministrazioni, delle Forze armate, delle forze di polizia o di enti pubblici per lo svolgimento dei suoi compiti istituzionali.

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

ORDINE DEL GIORNO

G5.100

MALLEGNI

Ritirato

Il Senato,

in sede di discussione 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;

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.

ARTICOLO 6 DEL DECRETO-LEGGE NEL TESTO COMPRENDENTE LE MODIFICAZIONI APPORTATE DALLA CAMERA DEI DEPUTATI

Articolo 6.

(Organizzazione dell'Agenzia per la cybersicurezza nazionale)

1. L'organizzazione e il funzionamento dell'Agenzia sono definiti da un apposito regolamento che ne prevede, in particolare, l'articolazione fino ad un numero massimo di otto uffici di livello dirigenziale generale, nonché fino ad un numero massimo di trenta articolazioni di livello dirigenziale non generale nell'ambito delle risorse finanziarie destinate all'Agenzia ai sensi dell'articolo 18, comma 1.

2. Sono organi dell'Agenzia il direttore generale e il Collegio dei revisori dei conti. Con il regolamento di cui al comma 1 sono disciplinati altresì:

a) le funzioni del direttore generale e del vice direttore generale dell'Agenzia;

b) la composizione e il funzionamento del Collegio dei revisori dei conti;

c) l'istituzione di eventuali sedi secondarie.

3. Il regolamento di cui al comma 1 è adottato, entro centoventi giorni dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, previo parere delle Commissioni parlamentari competenti per materia e per i profili finanziari e, per i profili di competenza, del COPASIR, sentito il CIC.

ORDINE DEL GIORNO

G6.100

MALLEGNI

Ritirato

Il Senato,

in sede di discussione 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;

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 Copasir, 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.

ARTICOLO 7 DEL DECRETO-LEGGE NEL TESTO COMPRENDENTE LE MODIFICAZIONI APPORTATE DALLA CAMERA DEI DEPUTATI

Articolo 7.

(Funzioni dell'Agenzia per la cybersicurezza nazionale)

1. L'Agenzia:

a) è Autorità nazionale per la cybersicurezza e, in relazione a tale ruolo, assicura, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni, ferme restando le attribuzioni del Ministro dell'interno in qualità di autorità nazionale di pubblica sicurezza, ai sensi della legge 1° aprile 1981, n. 121, il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore. Per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate restano fermi sia quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge n. 124 del 2007, sia le competenze dell'Ufficio centrale per la segretezza di cui all'articolo 9 della medesima legge n. 124 del 2007;

b) predispone la strategia nazionale di cybersicurezza;

c) svolge ogni necessaria attività di supporto al funzionamento del Nucleo per la cybersicurezza, di cui all'articolo 8;

d) è Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al decreto legislativo NIS, a tutela dell'unità giuridica dell'ordinamento, ed è competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto;

e) è Autorità nazionale di certificazione della cybersicurezza ai sensi dell'articolo 58 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni; nello svolgimento dei compiti di cui alla presente lettera:

1) accredita, ai sensi dell'articolo 60, paragrafo 1, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza;

2) delega, ai sensi dell'articolo 56, paragrafo 6, lettera *b)*, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, il Ministero della difesa e il Ministero dell'interno, attraverso le rispettive strutture accreditate di cui al numero 1) della presente lettera, al rilascio del certificato europeo di sicurezza cibernetica;

f) assume tutte le funzioni in materia di cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello sviluppo economico, ivi comprese quelle relative:

1) al perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le funzioni attribuite al Centro di valutazione e certificazione nazionale ai sensi del decreto-legge perimetro, le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera *c)*, del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131;

2) alla sicurezza e all'integrità delle comunicazioni elettroniche, di cui agli articoli 16-*bis* e 16-*ter* del decreto legislativo 1° agosto 2003, n. 259, e relative disposizioni attuative;

3) alla sicurezza delle reti e dei sistemi informativi, di cui al decreto legislativo NIS;

g) partecipa, per gli ambiti di competenza, al gruppo di coordinamento istituito ai sensi dei regolamenti di cui all'articolo 1, comma 8, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56;

h) assume tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera *c)*, del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri n. 131 del 2020;

i) assume tutte le funzioni già attribuite al Dipartimento delle informazioni per la sicurezza (DIS), di cui all'articolo 4 della legge 3 agosto 2007, n. 124, dal decreto-legge perimetro e dai relativi provvedimenti attuativi e supporta il Presidente del Consiglio dei ministri ai fini dell'articolo 1, comma 19-*bis*, del decreto-legge perimetro;

l) provvede, sulla base delle attività di competenza del Nucleo per la cybersicurezza di cui all'articolo 8, alle attività necessarie per l'attuazione e il controllo dell'esecuzione dei provvedimenti assunti dal Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro;

m) assume tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti e, in particolare, quelle di

cui all'articolo 51 del decreto legislativo 7 marzo 2005, n. 82, nonché quelle in materia di adozione di linee guida contenenti regole tecniche di cybersicurezza ai sensi dell'articolo 71 del medesimo decreto legislativo. L'Agenzia assume, altresì, i compiti di cui all'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, già attribuiti all'Agenzia per l'Italia digitale;

m-bis) assume le iniziative idonee a valorizzare la crittografia come strumento di cybersicurezza, anche attraverso un'apposita sezione dedicata nell'ambito della strategia di cui alla lettera *b)*. 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;

m-ter) provvede alla qualificazione dei servizi *cloud* per la pubblica amministrazione nel rispetto della disciplina dell'Unione europea e del regolamento di cui all'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221;

n) sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il CSIRT Italia di cui all'articolo 8 del decreto legislativo NIS. A tale fine, promuove iniziative di partenariato pubblico-privato, per rendere effettive tali capacità;

o) partecipa alle esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;

p) cura e promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale. A tal fine, l'Agenzia esprime pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la cybersicurezza;

q) coordina, in raccordo con il Ministero degli affari esteri e della cooperazione internazionale, la cooperazione internazionale nella materia della cybersicurezza. Nell'ambito dell'Unione europea e a livello internazionale, l'Agenzia cura i rapporti con i competenti organismi, istituzioni ed enti, nonché segue nelle competenti sedi istituzionali le tematiche di cybersicurezza, fatta eccezione per gli ambiti in cui la legge attribuisce specifiche competenze ad altre amministrazioni. In tali casi, è comunque assicurato il raccordo con l'Agenzia al fine di garantire posizioni nazionali unitarie e coerenti con le politiche di cybersicurezza definite dal Presidente del Consiglio dei ministri;

r) perseguendo obiettivi di eccellenza, supporta negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. A tali fini, l'Agenzia può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore. L'Agenzia as-

sicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti alla ricerca militare. L'Agenzia può altresì promuovere la costituzione di aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione e il reclutamento di personale nei settori avanzati dello sviluppo della cybersicurezza, nonché promuovere la realizzazione di studi di fattibilità e di analisi valutative finalizzati a tale scopo;

s) stipula accordi bilaterali e multilaterali, anche mediante il coinvolgimento del settore privato e industriale, con istituzioni, enti e organismi di altri Paesi per la partecipazione dell'Italia a programmi di cybersicurezza, assicurando il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale;

t) promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della cybersicurezza e dei correlati servizi applicativi, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti a progetti e iniziative in collaborazione con la NATO e con l'Agenzia europea per la difesa;

u) svolge attività di comunicazione e promozione della consapevolezza in materia di cybersicurezza, al fine di contribuire allo sviluppo di una cultura nazionale in materia;

v) promuove la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza, in particolare favorendo l'attivazione di percorsi formativi universitari in materia, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati; nello svolgimento di tali compiti, l'Agenzia può avvalersi anche delle strutture formative e delle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri interessati;

v-bis) può predisporre attività di formazione specifica riservate ai giovani che aderiscono al servizio civile regolate sulla base di apposite convenzioni. In ogni caso, il servizio prestato è, a tutti gli effetti, riconosciuto come servizio civile;

z) per le finalità di cui al presente articolo, può costituire e partecipare a partenariati pubblico-privato sul territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri.

aa) è designata quale Centro nazionale di coordinamento ai sensi dell'articolo 6 del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

1-*bis.* Anche ai fini dell'esercizio delle funzioni di cui al comma 1, lettere *r), s), t), u), v), z)* e *aa)*, presso l'Agenzia è istituito, con funzioni di consulenza e di proposta, un Comitato tecnico-scientifico, presieduto dal direttore generale della medesima Agenzia, o da un dirigente da lui delegato, e composto da personale della stessa Agenzia e da qualificati rappresentanti dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza, designati con decreto del Presidente del Consiglio dei ministri. La composizione e l'organizzazione del Comitato tecnico-scientifico sono disciplinate secondo le modalità e i criteri definiti dal regolamento di cui all'articolo 6, comma 1. Per la partecipazione al Comitato tecnico-scientifico non sono previsti gettoni di presenza, compensi o rimborsi di spese.

2. Nell'ambito dell'Agenzia sono nominati, con decreto del Presidente del Consiglio dei ministri, il rappresentante nazionale, e il suo sostituto, nel Consiglio di direzione del Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca, ai sensi dell'articolo 12 del regolamento (UE) 2021/887.

3. Il CSIRT italiano di cui all'articolo 8 del decreto legislativo NIS è trasferito presso l'Agenzia e assume la denominazione di: « CSIRT Italia ».

4. Il Centro di valutazione e certificazione nazionale, istituito presso il Ministero dello sviluppo economico, è trasferito presso l'Agenzia.

5. Nel rispetto delle competenze del Garante per la protezione dei dati personali, l'Agenzia, per le finalità di cui al presente decreto, consulta il Garante e collabora con esso, anche in relazione agli incidenti che comportano violazioni di dati personali. L'Agenzia e il Garante possono stipulare appositi protocolli d'intenti che definiscono altresì le modalità della loro collaborazione nell'ambito delle risorse disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica.

ORDINI DEL GIORNO

G7.100

MARILOTTI, D'ARIENZO (*)

Ritirato

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.

(*) Firma aggiunta in corso di seduta

G7.101

RAUTI, MALAN

Non posto in votazione (*)

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.

(*) Accolto dal Governo

G7.102

RAUTI, MALAN

Non posto in votazione (*)

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.

(*) Accolto dal Governo

G7.103

RAUTI, MALAN

Non posto in votazione (*)

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.

(*) Accolto dal Governo

G7.104

RAUTI, MALAN

Non posto in votazione (*)

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.

(*) Accolto dal Governo

G7.105

GARRUTI, PERILLI, SANTANGELO, TONINELLI

V. testo 2

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, convertito, 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 prote-

zione 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.

G7.105 (testo 2)

GARRUTI, PERILLI, SANTANGELO, TONINELLI

Non posto in votazione (*)

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 n. 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, convertito, 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;.

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.

(*) Accolto dal Governo

ARTICOLI DA 8 A 10 DEL DECRETO-LEGGE NEL TESTO COMPRENDENTE LE MODIFICAZIONI APPORTATE DALLA CAMERA DEI DEPUTATI

Articolo 8.

(Nucleo per la cybersicurezza)

1. Presso l'Agenzia è costituito, in via permanente, il Nucleo per la cybersicurezza, a supporto del Presidente del Consiglio dei ministri nella materia della cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

2. Il Nucleo per la cybersicurezza è presieduto dal direttore generale dell'Agenzia o, per sua delega, dal vice direttore generale ed è composto dal Consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del DIS, dell'Agenzia informazioni e sicurezza esterna (AISE), di cui all'articolo 6 della legge 3 agosto 2007, n. 124, dell'Agenzia

informazioni e sicurezza interna (AISI), di cui all'articolo 7 della legge n. 124 del 2007, di ciascuno dei Ministeri rappresentati nel CIC e del Dipartimento della protezione civile della Presidenza del Consiglio dei ministri. Per gli aspetti relativi alla trattazione di informazioni classificate il Nucleo è integrato da un rappresentante dell'Ufficio centrale per la segretezza di cui all'articolo 9 della legge n. 124 del 2007.

3. I componenti del Nucleo possono farsi assistere alle riunioni da altri rappresentanti delle rispettive amministrazioni in relazione alle materie oggetto di trattazione. In base agli argomenti delle riunioni possono anche essere chiamati a partecipare rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati alla materia della cybersicurezza.

4. Il Nucleo può essere convocato in composizione ristretta con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati, anche relativamente ai compiti di gestione delle crisi di cui all'articolo 10.

4-*bis*. Ai componenti del Nucleo non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.

Articolo 9.

(Compiti del Nucleo per la cybersicurezza)

1. Per le finalità di cui all'articolo 8, il Nucleo per la cybersicurezza svolge i seguenti compiti:

a) può formulare proposte di iniziative in materia di cybersicurezza del Paese, anche nel quadro del contesto internazionale in materia;

b) promuove, sulla base delle direttive di cui all'articolo 2, comma 2, la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale, in raccordo con le pianificazioni di difesa civile e di protezione civile, anche nel quadro di quanto previsto dall'articolo 7-*bis*, comma 5, del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198;

c) promuove e coordina lo svolgimento di esercitazioni interministeriali, ovvero la partecipazione nazionale a esercitazioni internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;

d) valuta e promuove, in raccordo con le amministrazioni competenti per specifici profili della cybersicurezza, procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi;

e) acquisisce, anche per il tramite del CSIRT Italia, le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi dagli organismi di informazione di cui agli articoli 4, 6 e 7 della legge 3 agosto

2007, n. 124, dalle Forze di polizia e, in particolare, dall'organo del Ministero dell'interno di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, dalle strutture del Ministero della difesa, nonché dalle altre amministrazioni che compongono il Nucleo e dai gruppi di intervento per le emergenze informatiche (*Computer Emergency Response Team* - CERT) istituiti ai sensi della normativa vigente;

f) riceve dal CSIRT Italia le notifiche di incidente ai sensi delle disposizioni vigenti;

g) valuta se gli eventi di cui alle lettere *e)* e *f)* assumono dimensioni, intensità o natura tali da non poter essere fronteggiati dalle singole amministrazioni competenti in via ordinaria, ma richiedono l'assunzione di decisioni coordinate in sede interministeriale, provvedendo in tal caso a informare tempestivamente il Presidente del Consiglio dei ministri, ovvero l'Autorità delegata, ove istituita, sulla situazione in atto e allo svolgimento delle attività di raccordo e coordinamento di cui all'articolo 10, nella composizione ivi prevista.

Articolo 10.

(Gestione delle crisi che coinvolgono aspetti di cybersicurezza)

1. Nelle situazioni di crisi che coinvolgono aspetti di cybersicurezza, nei casi in cui il Presidente del Consiglio dei ministri convochi il CISR in materia di gestione delle predette situazioni di crisi, alle sedute del Comitato sono chiamati a partecipare il Ministro delegato per l'innovazione tecnologica e la transizione digitale e il direttore generale dell'Agenzia.

3. In situazioni di crisi di natura cibernetica il Nucleo è integrato, in ragione della necessità, con un rappresentante, rispettivamente, del Ministero della salute e del Ministero dell'interno-Dipartimento dei Vigili del fuoco, del soccorso pubblico e della difesa civile, in rappresentanza anche della Commissione interministeriale tecnica di difesa civile, autorizzati ad assumere decisioni che impegnano la propria amministrazione. Alle riunioni i componenti possono farsi accompagnare da altri funzionari della propria amministrazione. Alle stesse riunioni possono essere chiamati a partecipare rappresentanti di altre amministrazioni, anche locali, ed enti, anche essi autorizzati ad assumere decisioni, e di altri soggetti pubblici o privati eventualmente interessati. Per la partecipazione non sono previsti compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.

4. È compito del Nucleo, nella composizione per la gestione delle crisi, di cui al comma 3, assicurare che le attività di reazione e stabilizzazione di competenza delle diverse amministrazioni ed enti rispetto a situazioni di crisi di natura cibernetica vengano espletate in maniera coordinata secondo quanto previsto dall'articolo 9, comma 1, lettera *b)*.

5. Il Nucleo, per l'espletamento delle proprie funzioni e fermo restando quanto previsto ai sensi dell'articolo 7-*bis*, comma 5, del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198:

a) mantiene costantemente informato il Presidente del Consiglio dei ministri, ovvero l'Autorità delegata, ove istituita, sulla crisi in atto, predisponendo punti aggiornati di situazione;

b) assicura il coordinamento per l'attuazione a livello interministeriale delle determinazioni del Presidente del Consiglio dei ministri per il superamento della crisi;

c) raccoglie tutti i dati relativi alla crisi;

d) elabora rapporti e fornisce informazioni sulla crisi e li trasmette ai soggetti pubblici e privati interessati;

e) partecipa ai meccanismi europei di gestione delle crisi cibernetiche, assicurando altresì i collegamenti finalizzati alla gestione della crisi con gli omologhi organismi di altri Stati, della NATO, dell'Unione europea o di organizzazioni internazionali di cui l'Italia fa parte.

ORDINI DEL GIORNO

G10.100

RAUTI, MALAN

V. testo 2

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.

G10.100 (testo 2)

RAUTI, MALAN

Non posto in votazione (*)

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, compatibilmente con gli equilibri di finanza pubblica.

(*) Accolto dal Governo

G10.101

RAUTI, MALAN

Non posto in votazione (*)

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

per cento 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 per cento;

secondo i dati in possesso della Polizia Postale, gli attacchi informatici in Italia sono aumentati del 246 per cento 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.

(*) Accolto dal Governo

G10.102

RAUTI, MALAN

Non posto in votazione (*)

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 per cento 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.

(*) Accolto dal Governo

G10.103

RAUTI, MALAN

V. testo 2

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 cibernetico 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.

G10.103 (testo 2)

RAUTI, MALAN

Non posto in votazione (*)

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 cibernetico 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, per imprese operanti in settori strategici e Pubblica Amministrazione, l'adozione di 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.

(*) Accolto dal Governo

G10.104

RAUTI, MALAN

Non posto in votazione (*)

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 Infrastructure 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 descritti 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.

(*) Accolto dal Governo

G10.105

BINETTI

V. testo 2

Il Senato,

in sede di discussione 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.

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, che possono 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 sanità 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 tecnico 77 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 *start up* 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.

G10.105 (testo 2)

BINETTI

Non posto in votazione (*)

Il Senato,

in sede di discussione 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.

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, che possono 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 sanità 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 tecnico 77 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 *start up* 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, compatibilmente con gli equilibri di finanza pubblica.

(*) Accolto dal Governo

ARTICOLO 11 DEL DECRETO-LEGGE NEL TESTO COMPRENDENTE LE MODIFICAZIONI APPORTATE DALLA CAMERA DEI DEPUTATI

Articolo 11.

(Norme di contabilità e disposizioni finanziarie)

1. Con la legge di bilancio è determinato lo stanziamento annuale da assegnare all'Agenzia da iscrivere sul capitolo di cui all'articolo 18, comma 1, sulla base della determinazione del fabbisogno annuo operata dal Presidente del Consiglio dei ministri, previamente comunicata al COPASIR.

2. Le entrate dell'Agenzia sono costituite da:

a) dotazioni finanziarie e contributi ordinari di cui all'articolo 18 del presente decreto;

b) corrispettivi per i servizi prestati a soggetti pubblici o privati;

c) proventi derivanti dallo sfruttamento della proprietà industriale, dei prodotti dell'ingegno e delle invenzioni dell'Agenzia;

d) altri proventi patrimoniali e di gestione;

e) contributi dell'Unione europea o di organismi internazionali, anche a seguito della partecipazione a specifici bandi, progetti e programmi di collaborazione;

f) proventi delle sanzioni irrogate dall'Agenzia ai sensi di quanto previsto dal decreto legislativo NIS, dal decreto-legge perimetro e dal decreto legislativo 1° agosto 2003, n. 259, e relative disposizioni attuative;

g) ogni altra eventuale entrata.

3. 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 e nel rispetto dei princìpi fondamentali da esse stabiliti, nonché delle seguenti disposizioni:

a) il bilancio preventivo e il bilancio consuntivo adottati dal direttore generale dell'Agenzia sono approvati con decreto del Presidente del Consiglio dei ministri, previo parere del CIC, e sono trasmessi alla Corte dei conti che esercita il controllo previsto dall'articolo 3, comma 4, della legge 14 gennaio 1994, n. 20;

b) il bilancio consuntivo e la relazione della Corte dei conti sono trasmessi alle Commissioni parlamentari competenti e al COPASIR.

4. Con regolamento adottato con decreto del Presidente del Consiglio dei ministri, su proposta del direttore generale dell'Agenzia, 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 in materia di contratti pubblici, previo parere del COPASIR e sentito il CIC, sono definite le procedure per la stipula di contratti di appalti di lavori e forniture di beni e servizi per le attività dell'Agenzia finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico, ferma restando la disciplina dell'articolo 162 del codice dei contratti pubblici relativi a lavori, servizi e forniture, di cui al decreto legislativo 18 aprile 2016, n. 50.

ORDINE DEL GIORNO

G11.100

MALLEGNI

Ritirato

Il Senato,

in sede di discussione 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;

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.

ARTICOLO 12 DEL DECRETO-LEGGE NEL TESTO COMPRENDENTE LE MODIFICAZIONI APPORTATE DALLA CAMERA DEI DEPUTATI

Articolo 12.

(Personale)

1. Con apposito regolamento è dettata, nel rispetto dei princìpi generali dell'ordinamento giuridico, anche in deroga alle vigenti disposizioni di legge, ivi incluso il decreto legislativo 30 marzo 2001, n. 165, e nel rispetto dei criteri di cui al presente decreto, la disciplina del contingente di personale addetto all'Agenzia, tenuto conto delle funzioni volte alla tutela della sicurezza nazionale nello spazio cibernetico attribuite all'Agenzia. Il regolamento definisce l'ordinamento e il reclutamento del personale, e il relativo trattamento economico e previdenziale, prevedendo, in particolare, per il personale dell'Agenzia di cui al comma 2, lettera *a)*, un trattamento economico pari a quello in godimento da parte dei dipendenti della Banca d'Italia, sulla scorta della equiparabilità delle funzioni svolte e del livello di responsabilità rivestito. La predetta equiparazione, con riferimento sia al trattamento economico in servizio che al trattamento previdenziale, produce effetti avendo riguardo alle anzianità di servizio maturate a seguito dell'inquadramento nei ruoli dell'Agenzia.

2. Il regolamento determina, nell'ambito delle risorse finanziarie destinate all'Agenzia ai sensi dell'articolo 18, comma 1, in particolare:

a) l'istituzione di un ruolo del personale e la disciplina generale del rapporto d'impiego alle dipendenze dell'Agenzia;

b) 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;

c) 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 cybersi-

curezza 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;

d) la determinazione della percentuale massima dei dipendenti che è possibile assumere a tempo determinato;

e) la possibilità di impiegare personale del Ministero della difesa, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri;

f) le ipotesi di incompatibilità;

g) le modalità di progressione di carriera all'interno dell'Agenzia;

h) la disciplina e il procedimento per la definizione degli aspetti giuridici e, limitatamente ad eventuali compensi accessori, economici del rapporto di impiego del personale oggetto di negoziazione con le rappresentanze del personale;

i) le modalità applicative delle disposizioni del decreto legislativo 10 febbraio 2005, n. 30, recante il Codice della proprietà industriale, ai prodotti dell'ingegno ed alle invenzioni dei dipendenti dell'Agenzia;

l) i casi di cessazione dal servizio del personale assunto a tempo indeterminato ed i casi di anticipata risoluzione dei rapporti a tempo determinato;

m) quali delle disposizioni possono essere oggetto di revisione per effetto della negoziazione con le rappresentanze del personale.

3. Qualora le assunzioni di cui al comma 2, lettera *b)*, riguardino professori universitari di ruolo o ricercatori universitari confermati si applicano le disposizioni di cui all'articolo 12 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, anche per quanto riguarda il collocamento in aspettativa.

4. In sede di prima applicazione delle disposizioni di cui al presente decreto, il numero di posti previsti dalla dotazione organica dell'Agenzia è individuato nella misura complessiva di trecento unità, di cui fino a un massimo di otto di livello dirigenziale generale, fino a un massimo di 24 di livello dirigenziale non generale e fino a un massimo di 268 unità di personale non dirigenziale.

5. Con decreti del Presidente del Consiglio dei ministri di concerto con il Ministro dell'economia e delle finanze, la dotazione organica può essere rideterminata nei limiti delle risorse finanziarie destinate alle spese per il personale di cui all'articolo 18, comma 1. Dei provvedimenti adottati in materia di dotazione organica dell'Agenzia è data tempestiva e motivata comunicazione alle Commissioni parlamentari competenti e al COPASIR.

6. Le assunzioni effettuate in violazione delle disposizioni del presente decreto o del regolamento di cui al presente articolo sono nulle, ferma restando la responsabilità personale, patrimoniale e disciplinare di chi le ha disposte.

7. Il personale che presta comunque la propria opera alle dipendenze o in favore dell'Agenzia è tenuto, anche dopo la cessazione di tale attività, al rispetto del segreto su ciò di cui sia venuto a conoscenza nell'esercizio o a causa delle proprie funzioni.

8. Il regolamento di cui al comma 1 è adottato, entro centoventi giorni dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, previo parere delle Commissioni parlamentari competenti per materia e per i profili finanziari e, per i profili di competenza, del COPASIR e sentito il CIC.

ORDINE DEL GIORNO

G12.100

MALLEGNI

Ritirato

Il Senato,

in sede di discussione 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;

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 legi-

slativo 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.

ARTICOLI DA 13 A 19 DEL DECRETO-LEGGE NEL TESTO COMPRENDENTE LE MODIFICAZIONI APPORTATE DALLA CAMERA DEI DEPUTATI

Articolo 13.

(Trattamento dei dati personali)

1. Il trattamento dei dati personali svolto per finalità di sicurezza nazionale in applicazione del presente decreto è effettuato ai sensi dell'articolo 58, commi 2 e 3, del decreto legislativo 30 giugno 2003, n. 196.

Articolo 14.

(Relazioni annuali)

1. Entro il 30 aprile di ogni anno, il Presidente del Consiglio dei ministri trasmette al Parlamento una relazione sull'attività svolta dall'Agenzia nell'anno precedente, in materia di cybersicurezza nazionale.

2. Entro il 30 giugno di ogni anno, il Presidente del Consiglio dei ministri trasmette al COPASIR una relazione sulle attività svolte nell'anno precedente dall'Agenzia negli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico relativamente ai profili di competenza del Comitato.

Articolo 15.

(Modificazioni al decreto legislativo NIS)

1. Al decreto legislativo NIS, sono apportate le seguenti modificazioni:

a) all'articolo 1, comma 2, lettera *a)*, le parole: « strategia nazionale di sicurezza cibernetica » sono sostituite dalle seguenti: « strategia nazionale di cybersicurezza »;

b) all'articolo 1, comma 2, lettera *b)*, le parole: « delle autorità nazionali competenti » sono sostituite dalle seguenti: « dell'autorità nazionale competente NIS, delle autorità di settore »;

c) all'articolo 3, lettera *a)*, le parole da: « autorità competente NIS » a: « per settore, » sono sostituite dalle seguenti: « autorità nazionale competente NIS, l'autorità nazionale unica, competente »;

d) all'articolo 3, dopo la lettera *a)*, è inserita la seguente: « *a*-bis*)* autorità di settore, le autorità di cui all'articolo 7, comma 1, lettere da *a)* a *e)* »;

e) all'articolo 4, il comma 6 è sostituito dal seguente:

« *6.* L'elenco degli operatori di servizi essenziali identificati ai sensi del comma 1 è riesaminato e, se del caso, aggiornato su base regolare, e almeno ogni due anni dopo il 9 maggio 2018, con le seguenti modalità:

a) le autorità di settore, in relazione ai settori di competenza, propongono all'autorità nazionale competente NIS le variazioni all'elenco degli operatori dei servizi essenziali, secondo i criteri di cui ai commi 2 e 3;

b) le proposte sono valutate ed eventualmente integrate, d'intesa con le autorità di settore, dall'autorità nazionale competente NIS che, con propri provvedimenti, provvede alle variazioni dell'elenco degli operatori dei servizi essenziali, dandone comunicazione, in relazione ai settori di competenza, anche alle autorità di settore. »;

f) all'articolo 6, nella rubrica, le parole: « sicurezza cibernetica » sono sostituite dalla seguente: « cybersicurezza »; ai commi 1, 2 e 3, le parole: « sicurezza cibernetica » sono sostituite dalla seguente: « cybersicurezza »; al comma 4, le parole: « La Presidenza del Consiglio dei ministri » sono sostituite dalle seguenti: « L'Agenzia per la cybersicurezza » e le parole: « sicurezza cibernetica » sono sostituite dalla seguente: « cybersicurezza »;

g) l'articolo 7 è sostituito dal seguente:

« Art. 7. - *(Autorità nazionale competente e punto di contatto unico) - 1.* L'Agenzia per la cybersicurezza nazionale è designata quale autorità nazionale competente NIS per i settori e sottosettori di cui all'allegato II e per i servizi di cui all'allegato III. Sono designate quali autorità di settore:

a) il Ministero dello sviluppo economico, per il settore infrastrutture digitali, sottosettori IXP, DNS, TLD, nonché per i servizi digitali;

b) il Ministero delle infrastrutture e della mobilità sostenibili, per il settore trasporti, sottosettori aereo, ferroviario, per vie d'acqua e su strada;

c) il Ministero dell'economia e delle finanze, per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob, secondo modalità di collaborazione e di scambio di informazioni stabilite con decreto del Ministro dell'economia e delle finanze;

d) il Ministero della salute, per l'attività di assistenza sanitaria, come definita dall'articolo 3, comma 1, lettera *a)*, del decreto legislativo 4 marzo 2014, n. 38, prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso, e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità sanitarie territorialmente competenti, per le attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati dalle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza;

e) il Ministero della transizione ecologica per il settore energia, sottosettori energia elettrica, gas e petrolio;

f) il Ministero della transizione ecologica e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.

2. L'autorità nazionale competente NIS è responsabile dell'attuazione del presente decreto con riguardo ai settori di cui all'allegato II e ai servizi di cui all'allegato III e vigila sull'applicazione del presente decreto a livello nazionale, esercitando altresì le relative potestà ispettive e sanzionatorie.

3. L'Agenzia per la cybersicurezza nazionale è designata quale punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi.

4. Il punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera dell'autorità nazionale competente NIS con le autorità competenti degli altri Stati membri, nonché con il gruppo di cooperazione di cui all'articolo 10 e la rete di CSIRT di cui all'articolo 11.

5. Il punto di contatto unico collabora nel gruppo di cooperazione in modo effettivo, efficiente e sicuro con i rappresentanti designati dagli altri Stati.

6. L'Agenzia per la cybersicurezza nazionale, in qualità di autorità nazionale competente NIS e di punto di contatto unico, consulta, conformemente alla normativa vigente, l'autorità di contrasto ed il Garante per la protezione dei dati personali e collabora con essi.

7. La Presidenza del Consiglio dei ministri comunica tempestivamente alla Commissione europea la designazione del punto di contatto unico e quella dell'autorità nazionale competente NIS, i relativi compiti e qualsiasi ulteriore modifica. Alle designazioni sono assicurate idonee forme di pubblicità.

8. Agli oneri derivanti dal presente articolo, pari a 1.300.000 euro annui a decorrere dall'anno 2018, si provvede ai sensi dell'articolo 22. »;

h) all'articolo 8, comma 1, le parole da: « la Presidenza » a: « la sicurezza » sono sostituite dalle seguenti: « l'Agenzia per la cybersicurezza nazionale »;

i) l'articolo 9, comma 1, è sostituito dal seguente:

« *1.* Le autorità di settore collaborano con l'autorità nazionale competente NIS per l'adempimento degli obblighi di cui al presente decreto. A tal fine è istituito presso l'Agenzia per la cybersicurezza nazionale un Comitato tecnico di raccordo. Il Comitato è presieduto dall'autorità nazionale competente NIS ed è composto dai rappresentanti delle amministrazioni statali individuate quali autorità di settore e da rappresentanti delle Regioni e Province autonome in numero non superiore a due, designati dalle Regioni e Province autonome in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. L'organizzazione del Comitato è definita con decreto del Presidente del Consiglio dei ministri, sentita la Conferenza unificata. Per la partecipazione al Comitato tecnico di raccordo non sono previsti gettoni di presenza, compensi o rimborsi di spese. »;

l) all'articolo 12, comma 5, le parole da: « e, per conoscenza, » a: « NIS, » sono soppresse;

m) all'articolo 14, comma 4, le parole da: « e, per conoscenza, » a: « NIS, » sono soppresse;

n) all'articolo 19, comma 1, le parole: « dalle autorità competenti NIS » sono sostituite dalle seguenti: « dall'autorità nazionale competente NIS »;

o) all'articolo 19, il comma 2 è abrogato;

p) all'articolo 20, comma 1, le parole da: « Le autorità competenti NIS » a: « sono competenti » sono sostituite da: « L'autorità nazionale competente NIS è competente »;

q) all'allegato I:

1) al punto 1, dopo la lettera *d)* è aggiunta la seguente: « *d-bis)* il CSIRT Italia conforma i propri servizi e la propria attività alle migliori pratiche internazionalmente riconosciute in materia di prevenzione, gestione e risposta rispetto a eventi di natura cibernetica »;

2) al punto 2, lettera *c)*, dopo la parola: « standardizzate » sono inserite le seguenti: « , secondo le migliori pratiche internazionalmente riconosciute, ».

2. Nel decreto legislativo NIS:

a) ogni riferimento al Ministero dello sviluppo economico, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale, fatta eccezione per le disposizioni di cui all'articolo 7, comma 1, lettera *a)*, del medesimo decreto legislativo, come sostituito dal comma 1, lettera *g)*, del presente articolo;

b) ogni riferimento al DIS, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale;

c) ogni riferimento alle autorità competenti NIS, ovunque ricorra, deve intendersi riferito all'autorità nazionale competente NIS, fatta eccezione per le disposizioni di cui all'articolo 5, comma 1, del medesimo decreto legislativo, come modificato dalla lettera *d)* del presente comma;

d) all'articolo 5, comma 1, alinea, le parole: « le autorità competenti NIS » sono sostituite dalle seguenti: « l'autorità nazionale competente NIS e le autorità di settore »;

e) agli articoli 6 e 12, le parole: « Comitato interministeriale per la sicurezza della Repubblica (CISR) » sono sostituite dalle seguenti: « Comitato interministeriale per la cybersicurezza (CIC) ».

Articolo 16.

(Altre modificazioni)

1. All'articolo 3, comma 1-*bis*, della legge 3 agosto 2007, n. 124, dopo le parole: « della presente legge » sono aggiunte le seguenti: « e in materia di cybersicurezza ».

2. All'articolo 38 della legge n. 124 del 2007, il comma 1-*bis* è abrogato a decorrere dal 1° gennaio 2023.

3. La denominazione: « CSIRT Italia » sostituisce, ad ogni effetto e ovunque presente in provvedimenti legislativi e regolamentari, la denominazione: « CSIRT Italiano ».

4. Nel decreto-legge perimetro le parole: « Comitato interministeriale per la sicurezza della Repubblica (CISR) » e « CISR », ovunque ricorrano, sono rispettivamente sostituite dalle seguenti: « Comitato interministeriale per la cybersicurezza (CIC) » e « CIC », fatta eccezione per le disposizioni di cui all'articolo 5 del medesimo decreto-legge.

5. Nel decreto-legge perimetro ogni riferimento al Dipartimento delle informazioni per la sicurezza, o al DIS, ovunque ricorra, è da intendersi riferito all'Agenzia per la cybersicurezza nazionale, fatta eccezione per le disposizioni dell'articolo 1, commi 2, lettera *b)*, e 2-*ter*, del medesimo decreto-legge perimetro, e ogni riferimento al Nucleo per la sicurezza cibernetica è da intendersi riferito al Nucleo per la cybersicurezza.

6. Nel decreto-legge perimetro:

a) ogni riferimento al Ministero dello sviluppo economico e alla Presidenza del Consiglio dei ministri, ovunque ricorra, è da intendersi riferito all'Agenzia per la cybersicurezza nazionale;

b) all'articolo 1, comma 8, lettera *a)*, le parole da: « definite dalla Presidenza del Consiglio dei ministri » a: « decreto legislativo 18 maggio 2018, n. 65 » sono sostituite dalle seguenti: « definite dall'Agenzia per la cybersicurezza nazionale »;

c) all'articolo 1, comma 8, lettera *b)*, le parole: « all'autorità competente » sono sostituite dalle seguenti: « autorità nazionale competente NIS ».

7. Nei provvedimenti di natura regolamentare e amministrativa la cui adozione è prevista dall'articolo 1 del decreto-legge perimetro, ogni riferimento al CISR e al DIS deve intendersi rispettivamente riferito al CIC e all'Agenzia per la cybersicurezza nazionale.

8. Nei provvedimenti di natura regolamentare e amministrativa la cui adozione è prevista dall'articolo 1 del decreto-legge perimetro, ogni riferimento al Ministero dello sviluppo economico e alla struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale, fatta eccezione per le disposizioni di cui all'articolo 3 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131.

9. Al decreto-legge perimetro sono apportate le seguenti modificazioni:

a) all'articolo 1, comma 6, lettera *a)*, dopo il primo periodo è inserito il seguente: « L'obbligo di comunicazione di cui alla presente lettera è efficace a decorrere dal trentesimo giorno successivo alla pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana del decreto del Presidente del Consiglio dei ministri che, sentita l'Agenzia per la cybersicurezza nazionale, attesta l'operatività del CVCN e comunque dal 30 giugno 2022. »;

a-bis) all'articolo 1, comma 7, lettera *c)*, le parole: « dell'organismo tecnico di supporto al CISR » sono sostituite dalle seguenti: « del Tavolo interministeriale di cui all'articolo 6 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131 »;

a-ter) all'articolo 1, comma 2, la lettera *b)* è sostituita dalla seguente:

« *b)* sono definiti, sulla base di un'analisi del rischio e di un criterio di gradualità che tenga conto delle specificità dei diversi settori di attività, i criteri con i quali i soggetti di cui al comma 2-*bis* predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, fermo restando che, per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate, si applica quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge 3 agosto 2007, n. 124; all'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, il Tavolo interministeriale di cui all'articolo 6 del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; entro sei mesi dalla data della comunicazione, prevista dal comma 2-*bis*, a ciascuno dei soggetti iscritti nell'elenco di cui al medesimo comma, i soggetti pubblici e quelli di cui all'articolo 29 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, nonché quelli privati, di cui al citato comma 2-*bis*, trasmettono tali elenchi all'Agenzia per la cybersicurezza nazionale, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la cybersicurezza; il Dipartimento delle informazioni per la sicurezza, l'Agenzia informazioni e sicurezza esterna (AISE) e l'Agenzia informazioni e sicurezza interna (AISI) ai fini dell'esercizio delle funzioni istituzionali previste dagli articoli 1, comma 3-*bis*, 4, 6 e 7 della legge n. 124 del 2007, nonché l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155*,* accedono a tali elenchi per il tramite della piattaforma digitale di cui all'articolo 9, comma 1, del regolamento di cui al

decreto del Presidente del Consiglio dei ministri n. 131 del 2020, costituita presso l'Agenzia per la cybersicurezza nazionale »;

a-quater) all'articolo 1, dopo il comma 2-*bis* è inserito il seguente:

« *2-ter*. Gli elenchi dei soggetti di cui alla lettera *a)* del comma 2 del presente articolo sono trasmessi al Dipartimento delle informazioni per la sicurezza, che provvede anche a favore dell'AISE e dell'AISI ai fini dell'esercizio delle funzioni istituzionali previste dagli articoli 1, comma 3-*bis*, 4, 6 e 7 della legge 3 agosto 2007, n. 124 »;

b) all'articolo 3, il comma 2 è abrogato;

c) a decorrere dalla data in cui diviene efficace l'obbligo di comunicazione disciplinato dalla lettera *a)*, all'articolo 3:

1) il comma 1 è sostituito dal seguente: « *1*. I soggetti che intendono procedere all'acquisizione, a qualsiasi titolo, di beni, servizi e componenti di cui all'articolo 1-*bis*, comma 2, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, sono obbligati ad effettuare la comunicazione di cui all'articolo 1, comma 6, lettera *a)*, per lo svolgimento delle verifiche di sicurezza da parte del CVCN sulla base delle procedure, modalità e termini previsti dal regolamento di attuazione. Ai fornitori dei predetti beni, servizi e componenti si applica l'articolo 1, comma 6, lettera *b)*. »;

2) il comma 3 è abrogato;

10. A decorrere dalla data in cui diviene efficace l'obbligo di comunicazione disciplinato dal comma 9, lettera *a)*, al decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, il comma 3-*bis* dell'articolo 1-*bis* è sostituito dal seguente: « *3-bis.* Entro dieci giorni dalla conclusione di un contratto o accordo di cui al comma 2, l'impresa che ha acquisito, a qualsiasi titolo, i beni o i servizi di cui allo stesso comma notifica alla Presidenza del Consiglio dei ministri un'informativa completa, contenente anche la comunicazione del Centro di valutazione e certificazione nazionale (CVCN), relativa all'esito della valutazione e alle eventuali prescrizioni, in modo da consentire l'eventuale esercizio del potere di veto o l'imposizione di specifiche prescrizioni o condizioni. Qualora il contratto sia stato stipulato antecedentemente alla conclusione dei test imposti dal CVCN, il termine di cui al primo periodo decorre dalla comunicazione di esito positivo della valutazione effettuata dal CVCN. Entro trenta giorni dalla notifica, il Presidente del Consiglio dei ministri comunica l'eventuale veto ovvero l'imposizione di specifiche prescrizioni o condizioni. I poteri speciali sono esercitati nella forma dell'imposizione di specifiche prescrizioni o condizioni ogniqualvolta ciò sia sufficiente ad assicurare la tutela degli interessi essenziali della difesa e della sicurezza nazionale. Decorsi i predetti termini, i poteri speciali si intendono non esercitati. Qualora si renda necessario richiedere informazioni all'acquirente, tale termine è sospeso, per una sola volta, fino al ricevimento delle informazioni richieste, che sono rese entro il termine di dieci giorni. Qualora si renda necessario formulare richieste istruttorie a soggetti terzi, il predetto termine di trenta giorni è sospeso, per una sola volta,

fino al ricevimento delle informazioni richieste, che sono rese entro il termine di venti giorni. Le richieste di informazioni e le richieste istruttorie a soggetti terzi successive alla prima non sospendono i termini. In caso di incompletezza della notifica, il termine di trenta giorni previsto dal presente comma decorre dal ricevimento delle informazioni o degli elementi che la integrano. Fermo restando quanto previsto in materia di sanzioni al presente comma, nel caso in cui l'impresa notificante abbia iniziato l'esecuzione del contratto o dell'accordo oggetto della notifica prima che sia decorso il termine per l'esercizio dei poteri speciali, ovvero abbia eseguito il contratto o accordo in violazione del decreto di esercizio dei poteri speciali, il Governo può ingiungere all'impresa di ripristinare a proprie spese la situazione anteriore. Salvo che il fatto costituisca reato, chiunque non osservi gli obblighi di notifica di cui al presente articolo ovvero le disposizioni contenute nel provvedimento di esercizio dei poteri speciali è soggetto alla sanzione amministrativa pecuniaria del pagamento di una somma fino al 150 per cento del valore dell'operazione e comunque non inferiore al 25 per cento del medesimo valore. Nei casi di violazione degli obblighi di notifica di cui al presente articolo, anche in assenza della notifica, la Presidenza del Consiglio dei ministri può avviare il procedimento ai fini dell'eventuale esercizio dei poteri speciali. A tale scopo, trovano applicazione i termini e le norme procedurali previsti dal presente comma. Il termine di trenta giorni di cui al presente comma decorre dalla conclusione del procedimento di accertamento della violazione dell'obbligo di notifica ».

11. All'articolo 135, comma 1, del codice del processo amministrativo, di cui all'allegato 1 al decreto legislativo 2 luglio 2010, n. 104, dopo la lettera *h)*, è aggiunta la seguente: « *h-bis)* le controversie aventi ad oggetto i provvedimenti dell'Agenzia per la cybersicurezza nazionale; » e alla lettera *o*) le parole: « e dell'AISE » sono sostituite dalle seguenti: « , dell'AISE e dell'Agenzia per la cybersicurezza nazionale ».

12. Alla legge 22 aprile 2021, n. 53, sono apportate le seguenti modificazioni:

a) all'articolo 4, comma 1, lettera *b)*, dopo le parole: « Ministero dello sviluppo economico » sono aggiunte le seguenti: « e l'Agenzia per la cybersicurezza nazionale »;

b) all'articolo 18, ogni riferimento al Ministero dello sviluppo economico, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale.

13. All'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, le parole: « L'AgID » sono sostituite dalle seguenti: « L'Agenzia per la cybersicurezza nazionale » e sono aggiunte, in fine, le seguenti parole: « nonché le modalità del procedimento di qualificazione dei servizi *cloud* per la pubblica amministrazione ».

14. Al decreto legislativo 1° agosto 2003, n. 259, sono apportate le seguenti modificazioni:

a) agli articoli 16-*bis* e 16-*ter*, ogni riferimento al Ministero dello sviluppo economico, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale;

b) all'articolo 16-*ter*, comma 1, le parole: « Ministro dello sviluppo economico » sono sostituite dalle seguenti: « Presidente del Consiglio dei ministri »;

c) all'articolo 16-*ter*, comma 2, lettera *b)*, le parole: « , in collaborazione con gli Ispettorati territoriali del Ministero dello sviluppo economico, » sono soppresse.

Articolo 17.

(Disposizioni transitorie e finali)

1. Per lo svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, di cui all'articolo 7, l'Agenzia può provvedere, oltre che con proprio personale, con l'ausilio dell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

2. Per lo svolgimento delle funzioni relative all'attuazione e al controllo dell'esecuzione dei provvedimenti assunti da parte del Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro, l'Agenzia provvede con l'ausilio dell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

3. Il personale dell'Agenzia, nello svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, di cui all'articolo 7, nonché delle funzioni relative all'attuazione e al controllo dell'esecuzione dei provvedimenti assunti da parte del Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro, riveste la qualifica di pubblico ufficiale.

4. Il personale dell'Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni, riveste la qualifica di pubblico ufficiale. La trasmissione delle notifiche di incidente ricevute dal CSIRT Italia all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, costituisce adempimento dell'obbligo di cui all'articolo 331 del codice di procedura penale.

5. Con uno o più decreti del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, da adottare entro centottanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, sono definiti i termini e le modalità:

a) per assicurare la prima operatività dell'Agenzia, mediante l'individuazione di appositi spazi, in via transitoria e per un massimo di ventiquattro mesi, secondo opportune intese con le amministrazioni interessate, per l'attuazione delle disposizioni del presente decreto;

b) mediante opportune intese con le amministrazioni interessate, nel rispetto delle specifiche norme riguardanti l'organizzazione e il funzionamento, per il trasferimento delle funzioni di cui all'articolo 7, nonché per il trasferimento dei beni strumentali e della documentazione, anche di natura classificata, per l'attuazione delle disposizioni del presente decreto e la corrispondente riduzione di risorse finanziarie ed umane da parte delle amministrazioni cedenti.

5-*bis*. Fino alla scadenza dei termini indicati nel decreto o nei decreti di cui al comma 5, lettera *b)*, la gestione delle risorse finanziarie relative alle funzioni trasferite, compresa la gestione dei residui passivi e perenti, è esercitata dalle amministrazioni cedenti. A decorrere dalla medesima data sono trasferiti in capo all'Agenzia i rapporti giuridici attivi e passivi relativi alle funzioni trasferite.

6. In relazione al trasferimento delle funzioni di cui all'articolo 7, comma 1, lettera *m*), dall'AgID all'Agenzia, i decreti di cui al comma 5 definiscono, altresì, i raccordi tra le due amministrazioni, per le funzioni che restano di competenza dell'AgID. Nelle more dell'adozione dei decreti di cui al comma 5, il regolamento di cui all'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, è adottato dall'AgID, d'intesa con la competente struttura della Presidenza del Consiglio dei ministri.

7. Al fine di assicurare la prima operatività dell'Agenzia, il direttore generale dell'Agenzia, fino all'adozione dei regolamenti di cui all'articolo 11, commi 3 e 4, identifica, assume e liquida gli impegni di spesa che verranno pagati a cura del DIS, nell'ambito delle risorse destinate all'Agenzia. A tale fine è istituito un apposito capitolo nel bilancio del DIS. Entro 90 giorni dall'approvazione dei regolamenti di cui all'articolo 11, commi 3 e 4, il Presidente del Consiglio dei ministri dà informazione al COPASIR delle spese effettuate ai sensi del presente comma.

8. Al fine di assicurare la prima operatività dell'Agenzia, dalla data della nomina del direttore generale dell'Agenzia e nel limite del 30 per cento della dotazione organica complessiva iniziale di cui all'articolo 12, comma 4:

a) il DIS mette a disposizione il personale impiegato nell'ambito delle attività relative allo svolgimento delle funzioni oggetto di trasferimento, con modalità da definire mediante intese con lo stesso Dipartimento;

b) l'Agenzia si avvale, altresì, di unità di personale appartenenti al Ministero dello sviluppo economico, all'Agenzia per l'Italia digitale, ad altre pubbliche amministrazioni e ad autorità indipendenti, per un periodo massimo di sei mesi, prorogabile una sola volta per un massimo di ulteriori sei mesi, messo a disposizione dell'Agenzia stessa su specifica richiesta e secondo modalità individuate mediante intese con le rispettive amministrazioni di appartenenza.

8-*bis*. Gli oneri derivanti dall'attuazione del comma 8 restano a carico dell'amministrazione di appartenenza.

9. Il regolamento di cui all'articolo 12, comma 1, prevede apposite modalità selettive per l'inquadramento, nella misura massima del 50 per cento della dotazione organica complessiva, del personale di cui al comma 8 del presente articolo e del personale di cui all'articolo 12, comma 2, lettera *b)*, ove già appartenente alla pubblica amministrazione, nel contingente di personale addetto all'Agenzia di cui al medesimo articolo 12, che tengano conto delle mansioni svolte e degli incarichi ricoperti durante il periodo di servizio presso l'Agenzia, nonché delle competenze possedute e dei requisiti di professionalità ed esperienza richiesti per le specifiche posizioni. Il personale di cui al comma 8, lettera *a)*, è inquadrato, a decorrere dal 1° gennaio 2022, nel ruolo di cui all'articolo 12, comma 2, lettera *a)*, secondo le modalità definite dal regolamento di cui all'articolo 12, comma 1. Gli inquadramenti conseguenti alle procedure selettive di cui al presente comma, relative al personale di cui al comma 8, lettera *b)*, decorrono allo scadere dei sei mesi o della relativa proroga e, comunque, non oltre il 30 giugno 2022.

10. L'Agenzia si avvale del patrocinio dell'Avvocatura dello Stato, ai sensi dell'articolo 1 del testo unico approvato con regio decreto 30 ottobre 1933, n. 1611.

10-*bis*. In sede di prima applicazione del presente decreto:

a) la prima relazione di cui all'articolo 14, comma 1, è trasmessa entro il 30 novembre 2022;

b) entro il 31 ottobre 2022, il Presidente del Consiglio dei ministri trasmette alle Camere una relazione che dà conto dello stato di attuazione, al 30 settembre 2022, delle disposizioni di cui al presente decreto, anche al fine di formulare eventuali proposte in materia.

10-*ter*. I pareri delle Commissioni parlamentari competenti per materia e per i profili finanziari e del COPASIR previsti dal presente decreto sono resi entro il termine di trenta giorni dalla trasmissione dei relativi schemi di decreto, decorso il quale il Presidente del Consiglio dei ministri può comunque procedere all'adozione dei relativi provvedimenti.

Articolo 18.

(Disposizioni finanziarie)

1. Per l'attuazione degli articoli da 5 a 7 è istituito, nello stato di previsione del Ministero dell'economia e delle finanze, un apposito capitolo con una dotazione di 2.000.000 di euro per l'anno 2021, 41.000.000 di euro per l'anno 2022, 70.000.000 di euro per l'anno 2023, 84.000.000 di euro per l'anno 2024, 100.000.000 di euro per l'anno 2025, 110.000.000 di euro per l'anno 2026 e 122.000.000 di euro annui a decorrere dall'anno 2027.

2. Agli oneri di cui al comma 1, si provvede mediante corrispondente riduzione del Fondo di cui all'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190.

3. Le risorse iscritte sui bilanci delle amministrazioni interessate, correlate alle funzioni ridefinite ai sensi del presente decreto a decorrere dall'inizio del funzionamento dell'Agenzia di cui all'articolo 5, sono accertate, anche in conto residui, con decreto del Ministro dell'economia e delle finanze, di concerto con i Ministri responsabili, e portate ad incremento del Fondo di cui all'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190, anche mediante versamento all'entrata del bilancio dello Stato e successiva riassegnazione alla spesa.

4. I proventi di cui all'articolo 11, comma 2, sono versati all'entrata del bilancio dello Stato, per essere riassegnati al capitolo di cui al comma 1 del presente articolo.

5. Ai fini dell'immediata attuazione delle disposizioni del presente decreto il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, anche in conto residui, le occorrenti variazioni di bilancio.

Articolo 19.

(*Entrata in vigore*)

1. Il presente decreto entra in vigore il giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana e sarà presentato alle Camere per la conversione in legge.

Allegato B

Parere espresso dalla 5a Commissione permanente sul testo del disegno di legge n. 2336

La Commissione programmazione economica, bilancio esaminato il disegno di legge in titolo, alla luce della relazione tecnica aggiornata, di cui all'articolo 17, comma 8, della legge di contabilità, positivamente verificata, esprime, per quanto di competenza, parere non ostativo.

VOTAZIONI QUALIFICATE EFFETTUATE NEL CORSO DELLA SEDUTA

VOTAZIONE		OGGETTO	RISULTATO						ESITO
Num.	Tipo		Pre	Vot	Ast	Fav	Cont	Magg	
1	Nom.	Disegno di legge n. 2336. Votazione finale	231	230	023	204	003	104	APPR.

- Le Votazioni annullate e quelle in cui è mancato il numero legale non sono riportate

(F)=Favorevole (C)=Contrario (A)=Astenuto (V)=Votante (s)=Subentrante (N)=Presente non Votante
(M)=Cong/Gov/Miss (P)=Presidente (R)=Richiedente la votazione e non votante

Nominativo	**1**
Abate Rosa Silvana	
Accoto Rossella	M
Agostinelli Donatella	F
Aimi Enrico	F
Airola Alberto	F
Alberti Casellati Maria Elisab	
Alderisi Francesca	M
Alessandrini Valeria	F
Alfieri Alessandro	F
Anastasi Cristiano	M
Angrisani Luisa	A
Arrigoni Paolo	F
Astorre Bruno	M
Auddino Giuseppe	F
Augussori Luigi	F
Bagnai Alberto	F
Balboni Alberto	M
Barachini Alberto	F
Barbaro Claudio	A
Barboni Antonio	
Battistoni Francesco	M
Bellanova Teresa	M
Berardi Roberto	
Bergesio Giorgio Maria	F
Bernini Anna Maria	F
Berutti Massimo Vittorio	F
Biasotti Sandro Mario	F
Binetti Paola	F
Bini Caterina	M
Biti Caterina	F
Boldrini Paola	F
Bongiorno Giulia	F
Bonifazi Francesco	M
Bonino Emma	F
Borghesi Stefano	F
Borgonzoni Lucia	M
Bossi Simone	F
Bossi Umberto	M
Bottici Laura	F
Botto Elena	

(F)=Favorevole (C)=Contrario (A)=Astenuto (V)=Votante (s)=Subentrante (N)=Presente non Votante

(M)=Cong/Gov/Miss (P)=Presidente (R)=Richiedente la votazione e non votante

Nominativo	**1**
Bressa Gianclaudio	F
Briziarelli Luca	M
Bruzzone Francesco	F
Buccarella Maurizio	F
Calandrini Nicola	M
Calderoli Roberto	F
Caliendo Giacomo	F
Caligiuri Fulvia Michela	M
Campagna Antonella	F
Campari Maurizio	F
Candiani Stefano	F
Candura Massimo	F
Cangini Andrea	F
Cantù Maria Cristina	F
Carbone Vincenzo	M
Cario Adriano	F
Casini Pier Ferdinando	F
Casolati Marzia	M
Castaldi Gianluca	F
Castellone Maria Domenica	F
Castiello Francesco	F
Catalfo Nunzia	F
Cattaneo Elena	M
Causin Andrea	M
Centinaio Gian Marco	M
Cerno Tommaso	M
Cesaro Luigi	F
Ciampolillo Alfonso	C
Cioffi Andrea	
Ciriani Luca	A
Cirinnà Monica	M
Collina Stefano	F
Coltorti Mauro	F
Comincini Eugenio Alberto	F
Conzatti Donatella	F
Corbetta Gianmarco	F
Corrado Margherita	A
Corti Stefano	F
Craxi Stefania Gabriella A.	F
Crimi Vito Claudio	F
Croatti Marco	F
Crucioli Mattia	A
Cucca Giuseppe Luigi Salvatore	M
Dal Mas Franco	F
D'Alfonso Luciano	F
Damiani Dario	F
D'Angelo Grazia	F

(F)=Favorevole (C)=Contrario (A)=Astenuto (V)=Votante (s)=Subentrante (N)=Presente non Votante
(M)=Cong/Gov/Miss (P)=Presidente (R)=Richiedente la votazione e non votante

Nominativo	**1**
D'Arienzo Vincenzo	F
De Bertoldi Andrea	A
De Bonis Saverio	
De Carlo Luca	A
De Falco Gregorio	
De Lucia Danila	F
De Petris Loredana	F
De Poli Antonio	F
De Siano Domenico	F
De Vecchis William	F
Dell'Olio Gianmauro	F
Dessì Emanuele	
Di Girolamo Gabriella	F
Di Marzio Luigi	M
Di Micco Fabio	
Di Nicola Primo	F
Di Piazza Stanislao	F
Donno Daniela	F
Doria Carlo	M
Drago Tiziana Carmela Rosaria	
Durnwalder Meinhard	F
Endrizzi Giovanni	M
Errani Vasco	
Evangelista Elvira Lucia	F
Faggi Antonella	F
Fantetti Raffaele	
Faraone Davide	F
Fattori Elena	
Fazzolari Giovanbattista	A
Fazzone Claudio	F
Fede Giorgio	F
Fedeli Valeria	F
Fenu Emiliano	F
Ferrara Gianluca	F
Ferrari Alan	F
Ferrazzi Andrea	F
Ferrero Roberta	F
Ferro Giuseppe Massimo	F
Floridia Barbara	M
Floris Emilio	F
Fregolent Sonia	F
Fusco Umberto	F
Galliani Adriano	M
Gallicchio Agnese	F
Gallone Maria Alessandra	F
Garavini Laura	F
Garnero Santanchè. Daniela	A

(F)=Favorevole (C)=Contrario (A)=Astenuto (V)=Votante (s)=Subentrante (N)=Presente non Votante

(M)=Cong/Gov/Miss (P)=Presidente (R)=Richiedente la votazione e non votante

Nominativo	**1**
Garruti Vincenzo	F
Gasparri Maurizio	F
Gaudiano Felicia	F
Ghedini Niccolò	M
Giacobbe Francesco	M
Giammanco Gabriella	F
Giannuzzi Silvana	A
Giarrusso Mario Michele	
Ginetti Nadia	M
Giro Francesco Maria	
Girotto Gianni Pietro	
Granato Bianca Laura	A
Grassi Ugo	F
Grasso Pietro	F
Grimani Leonardo	F
Guidolin Barbara	F
Iannone Antonio	A
Iori Vanna	M
Iwobi Tony Chike	F
La Mura Virginia	
La Pietra Patrizio Giacomo	A
La Russa Ignazio Benito Maria	P
L'Abbate Pasqua	F
Laforgia Francesco	F
Laniece Albert	F
Lannutti Elio	M
Lanzi Gabriele	F
Laus Mauro Antonio Donato	F
Leone Cinzia	F
Lezzi Barbara	A
Licheri Ettore Antonio	F
Lomuti Arnaldo	F
Lonardo Alessandrina	
Lorefice Pietro	F
Lucidi Stefano	F
Lunesu Michelina	M
Lupo Giulia	F
Maffoni Gianpietro	A
Magorno Ernesto	F
Maiorino Alessandra	F
Malan Lucio	A
Mallegni Massimo	F
Malpezzi Simona Flavia	F
Manca Daniele	F
Mangialavori Giuseppe Tommaso	F
Mantero Matteo	
Mantovani Maria Laura	F

(F)=Favorevole (C)=Contrario (A)=Astenuto (V)=Votante (s)=Subentrante (N)=Presente non Votante
(M)=Cong/Gov/Miss (P)=Presidente (R)=Richiedente la votazione e non votante

Nominativo	**1**
Marcucci Andrea	F
Margiotta Salvatore	F
Marilotti Giovanni	M
Marin Raffaella Fiormaria	F
Marinello Gaspare Antonio	F
Marino Mauro Maria	F
Martelli Carlo	C
Marti Roberto	F
Masini Barbara	F
Matrisciano Mariassunta	F
Mautone Raffaele	F
Merlo Ricardo Antonio	M
Messina Alfredo	
Messina Assunta Carmela	F
Mininno Cataldo	
Minuto Anna Carmela	F
Mirabelli Franco	F
Misiani Antonio	F
Modena Fiammetta	F
Moles Rocco Giuseppe	M
Mollame Francesco	M
Montani Enrico	F
Montevecchi Michela	F
Monti Mario	M
Moronese Vilma	A
Morra Nicola	A
Nannicini Tommaso	F
Napolitano Giorgio	M
Nastri Gaetano	A
Naturale Gisella	F
Nencini Riccardo	F
Nisini Tiziana	M
Nocerino Simona Nunzia	F
Nugnes Paola	
Ortis Fabrizio	M
Ostellari Andrea	F
Pacifico Marinella	
Pagano Nazario	F
Papatheu Urania Giulia Rosina	F
Paragone Gianluigi	C
Parente Annamaria	F
Paroli Adriano	F
Parrini Dario	F
Patuanelli Stefano	M
Pavanelli Emma	F
Pazzaglini Giuliano	F
Pellegrini Emanuele	F

(F)=Favorevole (C)=Contrario (A)=Astenuto (V)=Votante (s)=Subentrante (N)=Presente non Votante
(M)=Cong/Gov/Miss (P)=Presidente (R)=Richiedente la votazione e non votante

Nominativo	**1**
Pellegrini Marco	F
Pepe Pasquale	F
Pergreffi Simona	F
Perilli Gianluca	F
Perosino Marco	F
Pesco Daniele	F
Petrenga Giovanna	A
Petrocelli Vito Rosario	
Pianasso Cesare	F
Piano Renzo	
Piarulli Angela Anna Bruna	F
Pichetto Fratin Gilberto	F
Pillon Simone	F
Pinotti Roberta	F
Pirovano Daisy	F
Pirro Elisa	F
Pisani Giuseppe	F
Pisani Pietro	F
Pittella Giovanni Saverio	F
Pittoni Mario	F
Pizzol Nadia	F
Presutto Vincenzo	M
Pucciarelli Stefania	M
Puglia Sergio	M
Quagliariello Gaetano	F
Quarto Ruggiero	F
Rampi Roberto	F
Rauti Isabella	A
Renzi Matteo	M
Riccardi Alessandra	F
Ricciardi Sabrina	F
Richetti Matteo	F
Ripamonti Paolo	F
Rivolta Erica	F
Rizzotti Maria	F
Rojc Tatjana	F
Romagnoli Sergio	F
Romani Paolo	
Romano Iunio Valerio	F
Romeo Massimiliano	F
Ronzulli Licia	M
Rossi Mariarosaria	F
Rossomando Anna	F
Rubbia Carlo	
Rufa Gianfranco	F
Ruotolo Alessandro	F
Ruspandini Massimo	A

(F)=Favorevole (C)=Contrario (A)=Astenuto (V)=Votante (s)=Subentrante (N)=Presente non Votante
(M)=Cong/Gov/Miss (P)=Presidente (R)=Richiedente la votazione e non votante

Nominativo	**1**
Russo Loredana	M
Saccone Antonio	F
Salvini Matteo	
Santangelo Vincenzo	F
Santillo Agostino	F
Saponara Maria	F
Saviane Paolo	M
Sbrana Rosellina	F
Sbrollini Daniela	M
Schifani Renato	
Sciascia Salvatore	M
Segre Liliana	M
Serafini Giancarlo	F
Siclari Marco	M
Sileri Pierpaolo	F
Siri Armando	
Stabile Laura	F
Stefani Erika	M
Stefano Dario	F
Steger Dieter	F
Sudano Valeria Carmela Maria	
Taricco Giacomino	F
Taverna Paola	F
Testor Elena	F
Tiraboschi Maria Virginia	F
Toffanin Roberta	F
Toninelli Danilo	F
Tosato Paolo	F
Totaro Achille	
Trentacoste Fabrizio	F
Turco Mario	
Unterberger Juliane	F
Urraro Francesco	F
Urso Adolfo	A
Vaccaro Sergio	M
Valente Valeria	F
Vallardi Gianpaolo	F
Vanin Orietta	F
Vattuone Vito	F
Verducci Francesco	F
Vescovi Manuel	F
Vitali Luigi	F
Vono Gelsomina	F
Zaffini Francesco	
Zanda Luigi Enrico	F
Zuliani Cristiano	F

SEGNALAZIONI RELATIVE ALLE VOTAZIONI EFFETTUATE NEL CORSO DELLA SEDUTA

Nel corso della seduta è pervenuta al banco della Presidenza la seguente comunicazione:

DISEGNO DI LEGGE N. 2336:
sulla votazione finale, il senatore Errani avrebbe voluto esprimere un voto favorevole.

Congedi e missioni

Sono in congedo i senatori: Accoto, Alderisi, Anastasi, Astorre, Balboni, Barachini, Battistoni, Bellanova, Bini, Bonifazi, Borgonzoni, Bossi Umberto, Briziarelli, Calandrini, Caligiuri, Carbone, Cario, Casolati, Cattaneo, Causin, Centinaio, Cerno, Cirinnà, Cucca, De Poli, Di Marzio, Doria, Endrizzi, Floridia, Galliani, Ghedini, Giacobbe, Ginetti, Iori, Lannutti, Lunesu, Marilotti, Marin, Merlo, Messina Assunta Carmela, Moles, Mollame, Monti, Napolitano, Nisini, Ortis, Pichetto Fratin, Pirro, Presutto, Pucciarelli, Puglia, Renzi, Ronzulli, Russo, Saviane, Sbrollini, Sciascia, Segre, Siclari, Sileri, Vaccaro e Vanin.

Sono assenti per incarico avuto dal Senato i senatori: Arrigoni, Castiello, Fazzone, Magorno e Urso, per attività del Comitato parlamentare per la sicurezza della Repubblica.

Gruppi parlamentari, variazioni nella composizione

La senatrice Botto, con lettera in data 29 luglio 2021, ha comunicato di cessare di far parte del Gruppo parlamentare MoVimento 5 Stelle e di aderire al Gruppo Misto.

Commissioni permanenti, approvazione di documenti

La 10ª Commissione permanente (Industria, commercio, turismo), nella seduta del 22 luglio 2021, ha approvato una risoluzione, ai sensi dell'articolo 50, comma 2, del Regolamento, nell'ambito dell'affare assegnato sulla razionalizzazione, la trasparenza e la struttura di costo del mercato elettrico e sugli effetti in bolletta in capo agli utenti (*Doc*. XXIV, n. 50).

Il predetto documento è inviato al Ministro dello sviluppo economico.

Commissioni parlamentari, presentazione di relazioni

In data 30 luglio, a nome delle Commissioni riunite 3ª (Affari esteri, emigrazione) e 4ª (Difesa), i senatori Vescovi e Vattuone hanno presentato, ai sensi dell'articolo 50, comma 3, del Regolamento:

la relazione sulla risoluzione, approvata il 21 luglio 2021, a conclusione dell'esame dell'affare assegnato sulla Relazione analitica sulle missioni internazionali in corso e sullo stato degli interventi cooperazione allo sviluppo a sostegno dei processi di pace e di stabilizzazione, riferita all'anno 2020, anche al fine della relativa proroga per l'anno 2021, deliberata dal Consiglio dei ministri il 17 giugno 2021 (*Doc*. XXIV, n. 48-A);

la relazione sulla risoluzione, approvata il 21 luglio 2021, a conclusione dell'esame dell'affare assegnato sulla Deliberazione del Consiglio dei ministri in merito alla prosecuzione delle missioni internazionali in corso e alla partecipazione dell'Italia a ulteriori missioni internazionali per l'anno 2021, adottata il 17 giugno 2021 (*Doc*. XXIV, n. 49-A).

Commissione parlamentare di inchiesta sul gioco illegale e sulle disfunzioni del gioco pubblico, composizione e convocazione

Il Presidente del Senato ha chiamato a far parte della Commissione parlamentare di inchiesta sul gioco illegale e sulle disfunzioni del gioco pubblico i senatori: Stefano Borghesi, Stefano Candiani, Andrea Cangini, Andrea Cioffi, Marco Croatti, Andrea De Bertoldi, Stanislao Di Piazza, Giovanni Endrizzi, Albert Lanièce, Elio Lannutti, Arnaldo Lomuti, Michelina Lunesu, Matteo Mantero, Mauro Maria Marino, Anna Carmela Minuto, Franco Mirabelli, Enrico Montani, Fabrizio Ortis, Gianni Pittella e Roberta Toffanin.

La Commissione è convocata giovedì 5 agosto 2021, alle ore 8,30, per procedere alla sua costituzione.

Disegni di legge, annunzio di presentazione

Ministro degli affari esteri e della cooperazione internazionale
Ratifica ed esecuzione dell'Accordo tra il Governo della Repubblica italiana e il Centro internazionale per l'ingegneria genetica e la biotecnologia (ICGEB) relativo alle attività del Centro e alla sua Sede situata in Italia, con Allegato, fatto a Roma il 21 giugno 2021 (2341)
(presentato in data 30/07/2021);

ministro degli affari esteri e della cooperazione internazionale

Ratifica ed esecuzione dell'Accordo tra il Governo della Repubblica italiana e l'Organizzazione Europea di Diritto Pubblico riguardante lo stabilimento di un Ufficio in Italia, con Allegato, fatto a Roma il 23 giugno 2021 (2342)
(presentato in data 30/07/2021);

senatore Romagnoli Sergio
Riordino delle competenze dei comuni in materia di elettromagnetismo e insediamento urbanistico e territoriale degli impianti radioelettrici, di radiodiffusione e di telefonia mobile (2343)
(presentato in data 30/07/2021);

senatori Collina Stefano, Alfieri Alessandro, Astorre Bruno, Biti Caterina, Boldrini Paola, Cerno Tommaso, Comincini Eugenio, D'Alfonso Luciano, Fedeli Valeria, Ferrazzi Andrea, Giacobbe Francesco, Iori Vanna, Laus Mauro Antonio Donato, Manca Daniele, Margiotta Salvatore, Parrini Dario, Pinotti Roberta, Pittella Gianni, Rojc Tatjana, Stefano Dario, Taricco Mino, Vattuone Vito, Verducci Francesco
Misure per la promozione e il sostegno delle start-up e delle piccole e medie imprese innovative (2344)
(presentato in data 02/08/2021);

senatori Manca Daniele, Parrini Dario, Comincini Eugenio, Mirabelli Franco, Zanda Luigi, Ferrari Alan, Biti Caterina, Valente Valeria, Marcucci Andrea, Boldrini Paola, Pittella Gianni
Norme in materia di valorizzazione degli ambiti territoriali ottimali per l'esercizio in forma associata delle funzioni fondamentali dei comuni e dei distretti di cui al decreto legislativo 30 dicembre 1992, n. 502 (2345)
(presentato in data 03/08/2021);

senatori Comincini Eugenio, Parrini Dario, Manca Daniele, Zanda Luigi, Mirabelli Franco, Ferrari Alan, Biti Caterina, Marcucci Andrea, D'Alfonso Luciano
Norme in materia di riconoscimento degli oneri previdenziali, assistenziali e assicurativi in favore dei sindaci e degli amministratori locali (2346)
(presentato in data 03/08/2021);

senatori Guidolin Barbara, Matrisciano Susy, Catalfo Nunzia, Romagnoli Sergio, Romano Iunio Valerio, Trentacoste Fabrizio, Endrizzi Giovanni, Vanin Orietta, Lanzi Gabriele, Castellone Maria Domenica, Montevecchi Michela, Campagna Antonella, Pisani Giuseppe, Pavanelli Emma, Donno Daniela
Disposizioni per l'introduzione del personale infermieristico e degli operatori socio sanitari tra le categorie usuranti (2347)
(presentato in data 02/08/2021);

senatrice Saponara Maria
Celebrazioni per il centesimo anniversario della morte di Giacomo Puccini (2348)

(presentato in data 03/08/2021);

senatori Vallardi Gianpaolo, Bergesio Giorgio Maria, Sbrana Rosellina, Rufa Gianfranco, Zuliani Cristiano, Pisani Pietro, Iwobi Tony Chike, Pianasso Cesare
Disposizioni sulla istituzione dell'Albo degli agromeccanici e sull'esercizio dell'attività di agromeccanico (2349)
(presentato in data 03/08/2021);

senatori Cantù Maria Cristina, Nannicini Tommaso, Puglia Sergio
Interventi finalizzati a garantire un giusto ristoro in favore dei medici deceduti o che hanno riportato lesioni o infermità di tipo irreversibile a causa dell'infezione da SARS-CoV-2 (2350)
(presentato in data 03/08/2021);

senatori Bossi Simone, Briziarelli Luca
Misure di contrasto dei fenomeni di inquinamento ambientale da acque reflue industriali (2351)
(presentato in data 03/08/2021);

senatori Donno Daniela, Pavanelli Emma, Puglia Sergio, Castaldi Gianluca, Vanin Orietta, Vaccaro Sergio, Piarulli Angela Anna Bruna, Pellegrini Marco, Campagna Antonella, Romano Iunio Valerio, Russo Loredana, Pisani Giuseppe
Istituzione della Polizia forestale, ambientale e agroalimentare nell'ambito dell'Amministrazione della pubblica sicurezza (2352)
(presentato in data 03/08/2021).

Disegni di legge, assegnazione

In sede redigente

1ª Commissione permanente Affari Costituzionali
Sen. Candura Massimo ed altri
Disposizioni in materia di armi bianche (2228)
previ pareri delle Commissioni 2ª (Giustizia), 5ª (Bilancio)
(assegnato in data 03/08/2021);

2ª Commissione permanente Giustizia
Sen. Di Girolamo Gabriella
Ripristino degli uffici giudiziari soppressi ai sensi del decreto legislativo 7 settembre 2012, n. 155 (2258)
previ pareri delle Commissioni 1ª (Affari Costituzionali), 5ª (Bilancio), Commissione parlamentare questioni regionali
(assegnato in data 03/08/2021);

8ª Commissione permanente Lavori pubblici, comunicazioni

Sen. Vono Gelsomina
Modifica all'articolo 90 del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259, in materia di esproprio per le infrastrutture di reti di comunicazione nazionale ad alta velocità (2296)
previ pareri delle Commissioni 1ª (Affari Costituzionali), 2ª (Giustizia), 5ª (Bilancio)
(assegnato in data 03/08/2021);

12ª Commissione permanente Igiene e sanità
Sen. Ronzulli Licia
Disposizioni in materia di obbligatorietà vaccinale anti SARS-CoV-2 per il personale docente e non docente (2327)
previ pareri delle Commissioni 1ª (Affari Costituzionali), 2ª (Giustizia), 5ª (Bilancio), 7ª (Istruzione pubblica, beni culturali), Commissione parlamentare questioni regionali
(assegnato in data 03/08/2021).

Governo, trasmissione di atti e documenti

Con lettere in data 30 luglio 2021 il Ministero dell'interno, in adempimento a quanto previsto dall'articolo 141, comma 6, del decreto legislativo 8 agosto 2000, n. 267, ha comunicato gli estremi del decreto del Presidente della Repubblica concernente lo scioglimento del consiglio comunale di San Nicandro Garganico (Foggia), Seminara (Reggio Calabria), Camposano (Napoli), Colle di Tora (Rieti), Fagnano Olona (Varese) e Seveso (Monza-Brianza).

Il Ministro della salute, con lettera in data 30 luglio 2021, ha inviato, ai sensi dell'articolo 16 della legge 22 maggio 1978, n. 194, la relazione - per la parte di sua competenza - sullo stato di attuazione della medesima legge n. 194 del 1978, recante norme per la tutela sociale della maternità e sull'interruzione volontaria della gravidanza, relativa all'anno 2019.

Il predetto documento è deferito, ai sensi dell'articolo 34, comma 1, secondo periodo, del Regolamento, alla 2ª e alla 12ª Commissione permanente (*Doc*. XXXVII, n. 3).

Il Ministro della salute, con lettera in data 30 luglio 2021, ha inviato, ai sensi dell'articolo 8 della legge 14 dicembre 2000, n. 376, la relazione sullo stato di attuazione della medesima legge n. 376 del 2000, recante disciplina della tutela sanitaria delle attività sportive e della lotta contro il doping e sull'attività svolta dalla Commissione per la vigilanza ed il controllo sul doping e per la tutela della salute nelle attività sportive, riferita all'anno 2020.

Il predetto documento è deferito, ai sensi dell'articolo 34, comma 1, secondo periodo, del Regolamento, alla 7ª e alla 12ª Commissione permanente (*Doc*. CXXXV, n. 4).

Il Ministro della salute, con lettera in data 28 luglio 2021, ha inviato, ai sensi dell'articolo 3, comma 68, della legge 24 dicembre 2007, n. 244, la relazione sullo stato della spesa, sull'efficacia nell'allocazione delle risorse e sul grado di efficienza dell'azione amministrativa svolta dal Ministero della salute, riferita all'anno 2020.

Il predetto documento è deferito, ai sensi dell'articolo 34, comma 1, secondo periodo, del Regolamento, alla 1ª, alla 5ª e alla 12ª Commissione permanente (*Doc*. CLXIV, n. 34).

Il Ministro delle politiche agricole alimentari e forestali, con lettera in data 22 luglio 2021, ha trasmesso, ai sensi dell'articolo 1, comma 1075, della legge 27 dicembre 2017, n. 205, dell'articolo 1, comma 105, della legge 30 dicembre 2018, n. 145, e dell'articolo 1, comma 25, della legge 27 dicembre 2019, n. 160, la relazione concernente lo stato di avanzamento degli interventi di competenza del Ministero delle politiche agricole, alimentari e forestali finanziati con le risorse del fondo per gli investimenti e lo sviluppo infrastrutturale del Paese, di cui all'articolo 1, comma 140, della legge 11 dicembre 2016, n. 232, del fondo di cui all'articolo 1, comma 95, della legge 30 dicembre 2018, n. 145, e del fondo di cui all'articolo 1, comma 14, della legge 27 dicembre 2019, n. 160, aggiornata al 30 giugno 2021.

Il predetto documento è deferito, ai sensi dell'articolo 34, comma 1, secondo periodo, del Regolamento, alla 5ª, alla 8ª e alla 9ª Commissione permanente (*Doc*. CCXL, n. 10).

Governo, trasmissione di atti concernenti procedure d'infrazione

Il Ministro delle infrastrutture e delle mobilità sostenibili, con lettera in data 27 luglio 2021, ha trasmesso, in ottemperanza dell'articolo 15, comma 2, della legge 24 dicembre 2012, n. 234, la relazione sulla procedura d'infrazione n. 2021/2043, - avviata ai sensi dell'articolo 258 del Trattato sul funzionamento dell'Unione europea - relativa alla non corretta applicazione del Regolamento 2017/352 che istituisce un quadro normativo per la fornitura di servizi portuali e norme comuni in materia di trasparenza finanziaria dei porti.

Il predetto documento è deferito, ai sensi dell'articolo 34, comma 1, secondo periodo, del Regolamento, alla 8ª e alla 14ª Commissione permanente (Procedura d'infrazione n. 97/1).

Roma Capitale, trasmissione di documenti

Il Commissario straordinario del Governo per il piano di rientro del debito pregresso del Comune di Roma, con lettera in data 27 luglio 2021, ha inviato, ai sensi dell'articolo 14, comma 13-*quater*, del decreto-legge 31 maggio 2010, n. 78, convertito, con modificazioni, dalla legge 30 luglio 2010, n. 122, introdotto dall'articolo 13, comma 1, del decreto legislativo 18 aprile 2012, n. 61, le relazioni concernenti la rendicontazione delle attività svolte dalla gestione commissariale per il piano di rientro del debito pregresso di Roma Capitale, riferite agli anni 2018 (*Doc*. CC, n. 2), 2019 (*Doc*. CC, n. 3) e 2020 (*Doc*. CC, n. 4).

I predetti documenti sono deferiti, ai sensi dell'articolo 34, comma 1, secondo periodo, del Regolamento, alla 1ª e alla 5ª Commissione permanente.

Interrogazioni, apposizione di nuove firme

La senatrice La Mura ha aggiunto la propria firma all'interrogazione 4-05880 del senatore Lannutti e della senatrice Angrisani.

Il senatore Di Micco ha aggiunto la propria firma all'interrogazione 4-05881 del senatore Lannutti ed altri.

Mozioni

SAPONARA, PITTONI, ALESSANDRINI, ROMEO, FREGOLENT, MARIN, LUNESU, RUFA, RIVOLTA, FERRERO, FAGGI - Il Senato,

premesso che:

la legge 13 luglio 2015, n. 107 (detta "buona scuola"), ha valorizzato la formazione dei docenti, definendola obbligatoria, permanente e strutturale (comma 124 dell'art. 1). Ogni scuola a tal fine deve dotarsi di un piano di aggiornamento e formazione che definisca le attività di formazione dei docenti e del personale della scuola, in coerenza con il piano triennale dell'offerta formativa e con i risultati dei piani di miglioramento, sulla base delle priorità nazionali indicate nel piano nazionale per la formazione dei docenti, emanato ogni 3 anni dal Ministero dell'istruzione;

l'art. 282 del decreto legislativo 16 aprile 1994, n. 297, testo unico delle disposizioni legislative vigenti in materia di istruzione, relative alle

scuole di ogni ordine e grado, sancisce che l'aggiornamento è un diritto-dovere del personale ispettivo, direttivo e docente;

l'art. 27 del contratto collettivo nazionale di lavoro attualmente vigente, stabilisce che: "Il profilo professionale dei docenti è costituito da competenze disciplinari, informatiche, linguistiche, psicopedagogiche, metodologico-didattiche, organizzativo relazionali, di orientamento e di ricerca, documentazione e valutazione tra loro correlate ed interagenti, che si sviluppano col maturare dell'esperienza didattica, l'attività di studio e di sistematizzazione della pratica didattica. I contenuti della prestazione professionale del personale docente si definiscono nel quadro degli obiettivi generali perseguiti dal sistema nazionale di istruzione e nel rispetto degli indirizzi delineati nel piano dell'offerta formativa della scuola";

al di là dei riferimenti normativi, ogni docente che svolga il proprio lavoro in maniera responsabile dovrebbe considerare l'aggiornamento o la formazione come un'opportunità per migliorare e potenziare le proprie competenze e professionalità;

in materia di formazione, le tematiche su cui più spesso si nutrono dei dubbi attengono ai seguenti aspetti;

monte ore obbligatorio: non esiste un numero di ore obbligatorie a cui si deve far riferimento, lo ha ribadito il Ministero nella nota n. 25134 del 1° giugno 2017, dove appunto si evince che l'obbligatorietà non consiste nelle ore da svolgere, ma nel rispetto del contenuto del piano nazionale per la formazione dei docenti;

funzione del collegio dei docenti: ad esso spetta il compito di approvare un piano di formazione nel rispetto del POF e tenendo conto delle esigenze formative dei docenti, in modo da pianificare gli aspetti organizzativi delle attività di formazione dei docenti;

obbligo della formazione: il comma 124 dell'art. 1 della legge n. 107 non ha vincoli di ore annuali di formazione, che deve essere svolta durante il servizio dei docenti, in quanto l'obbligatorietà della formazione è strettamente legata al servizio orario dei docenti e non deve rappresentare un aggravio di orario, oltre a quello previsto dal contratto. Il dirigente scolastico può sanzionare il docente che non partecipa alla formazione solo ed esclusivamente se questa è stata deliberata dal collegio, in quanto si tratterebbe di inadempimento agli obblighi di servizio;

libera scelta dei corsi da seguire: ogni docente è libero di scegliere il corso di formazione da seguire sia nell'ambito di iniziative già previste e organizzate dall'istituto scolastico, che presso enti accreditati dal Ministero, a condizione che tale formazione sia coerente con gli indirizzi e gli obiettivi prefissati dal piano approvato. Il docente può anche decidere di aggiornarsi autonomamente mediante autocertificazione delle ore impiegate per lo studio di libri, materiale *on line*, articoli di quotidiani, fonti normative, riviste specializzate, potendo richiedere tuttavia un riconoscimento informale ai fini del piano di aggiornamento e formazione, approvato dall'istituto, secondo criteri individuati e indicati nel piano stesso;

nella relazione programmatica sulla partecipazione dell'Italia all'Unione europea per l'anno 2021, il documento di indirizzo strategico nel quale si indicano gli impegni politici e le azioni prioritarie che il Governo intende porre alla base del proprio impegno in Europa, si rileva l'intenzione di rafforzare il ruolo e la qualità dell'istruzione e della formazione per fornire un contributo alla costruzione della strategia europea "Education and training post 2020", con l'obiettivo di progredire ulteriormente nella creazione di uno "spazio europeo dell'istruzione", anche attraverso il miglioramento del sistema di sviluppo professionale continuo dei docenti e la valorizzare di iniziative che supportano l'innovazione e la digitalizzazione delle scuole, con particolare riferimento a progetti di formazione dei docenti e dei dirigenti scolastici, anche tramite progetti di consorzi regionali;

i due anni di pandemia e lo svolgimento delle lezioni in DAD hanno messo in luce molte carenze nell'aggiornamento degli insegnanti e non solo per quanto attiene alle competenze digitali. Dai dati delle rilevazioni INVALSI si rileva che numerosi docenti si sono limitati a riproporre *on line* il metodo d'insegnamento più tradizionale: lezione frontale, compiti, verifiche. La pandemia ha messo in luce che le competenze didattiche di troppi docenti si fermano ad un'unica modalità, la più vecchia, e sono perciò inadeguate. La sola conoscenza della materia non basta più, ma al centro va messa la capacità di insegnare: formazione, aggiornamento, innovazione didattica devono diventare un obbligo per tutti, neoassunti e già in servizio;

la prima parte del comma 124 dell'art. 1 della legge n. 107 del 2015 recita che: "Nell'ambito degli adempimenti connessi alla funzione docente, la formazione in servizio dei docenti di ruolo è obbligatoria, permanente e strutturale". Le attività di formazione sono definite dalle singole istituzioni scolastiche", questo significa che le modalità dell'aggiornamento le decide il collegio dei docenti, che, sul tema, spesso si orienta su attività basate sul "minimo sindacale", per non scontentare nessuno. È quindi un fenomeno perfettamente naturale, quello dell'elusione, e per questo motivo si ritiene che la questione della formazione dei docenti meriti di essere affrontata in maniera diversa, innovativa. Ad esempio si potrebbe istituire una figura terza, che sia in grado di valutare i reali bisogni formativi dell'insegnante, in modo tale che, di comune accordo con il docente, possa valutare un percorso formativo adeguato, da svolgere in un arco temporale ampio. Dall'analisi del singolo *curriculum*, dovrebbe essere negoziato che cosa, come e quanto ciascun docente debba fare in un anno scolastico per aggiornarsi, approfittando dell'offerta formativa del territorio, spesso ricca e gratuita per il docente; ovviamente questi "supervisori dei bisogni formativi" vanno a loro volta formati attraverso un percorso universitario ben definito o particolari specializzazioni,

impegna il Governo ad assumere iniziative urgenti in materia di formazione dei docenti, in linea con le indicazioni del PNRR e con gli impegni assunti dall'Italia nel contesto europeo, al fine di realizzare un sistema di formazione degli insegnanti continuo, obbligatorio e gratuito, tale da consentire un costante aggiornamento della classe docente nel nostro Paese, per formare

al meglio le nuove generazioni in un contesto culturale e scientifico in progressiva evoluzione.

(1-00409)

COLLINA, GIACOBBE, ALFIERI, D'ALFONSO, D'ARIENZO, FEDELI, FERRAZZI, IORI, LAUS, MANCA, MARGIOTTA, PINOTTI, PITTELLA, ROJC, TARICCO, VALENTE - Il Senato,

premesso che:

nei primi giorni di luglio l'amministratore delegato della Intel Corporation, terzo produttore a livello globale di semiconduttori, Patrick Gelsinger, ha preso parte a importanti incontri istituzionali con il Governo italiano, le istituzioni UE e i Governi di Francia e Germania, in cui ha manifestato interesse per la realizzazione in Europa di un impianto composto da 6 a 8 moduli, il costo di ciascuno dei quali è stimato tra 10 e 15 miliardi di dollari in circa 10 anni;

l'amministratore delegato della Intel Corporation, con dichiarazioni rese pubbliche ha, altresì, affermato che la scelta della collocazione di tale fabbrica sarebbe stata presa a breve, esprimendo un sentimento di forte ottimismo nei confronti dell'Italia, dovuto all'approvazione del piano nazionale di ripresa e resilienza, con i conseguenti investimenti nel quadro del dispositivo per la ripresa e la resilienza;

considerato che:

gli Stati Uniti, pionieri della microelettronica, hanno gradualmente ceduto nel corso degli ultimi 30 anni la *leadership* mondiale nella produzione dei semiconduttori e il vantaggio competitivo di cui disponevano, mantenendo un ruolo rilevante soltanto nell'ambito della ricerca e dello sviluppo svolto dalle loro aziende e università. Attualmente, *leader* mondiali nella produzione di semiconduttori sono la Taiwan semiconductor manifacturing corporation (TSMC) con una quota del 28 per cento, seguita dall'azienda taiwanese Umc, che detiene una quota del 13 per cento, dalla cinese Smic con una quota dell'11 per cento e dalla coreana Samsung con una quota del 10 per cento;

l'Unione europea è responsabile di circa il 10 per cento del mercato globale di semiconduttori, dal momento che le principali aziende produttrici nel mondo sono collocate prevalentemente fuori dall'Europa, a Taiwan, in Corea del Sud, negli Stati Uniti, in Giappone e in Cina, con un unico grande produttore europeo, STMictroelectronics, in undicesima posizione, con sedi in Italia e Francia;

in questi mesi si sta assistendo, per la prima volta, ad una grave carenza di offerta di semiconduttori a livello globale, rafforzata dall'aumento della domanda di oltre il 20 per cento a marzo 2021. Situazione che sta mettendo a repentaglio la disponibilità dei numerosi e fondamentali prodotti finiti

che necessitano di semiconduttori, quali *computer*, cellulari, dispositivi medici e veicoli;

la catena di approvvigionamento di semiconduttori è pertanto improvvisamente entrata al centro di scontri strategici e commerciali, in particolare tra Cina e Stati Uniti, tanto da spingere l'amministrazione americana a varare un pesante regime sanzionatorio che include tariffe, *iter* approvativi di fusioni e acquisizioni rafforzati, licenze per *joint venture* ed esportazioni di tecnologie avanzate, in risposta a continui furti di proprietà intellettuale, trasferimenti tecnologici forzati, spionaggi informatici e violazioni dell'OMC, con un impatto notevole sull'industria di semiconduttori mondiale;

gli Stati Uniti, in risposta alla grave carenza di offerta di semiconduttori a livello globale e alle tensioni strategiche, stanno adottando iniziative volte a rafforzare la propria autonomia strategica nell'approvvigionamento di semiconduttori e a spostare il baricentro della produzione mondiale di *chip*, al momento in Asia orientale, la più importante delle quali è il "Creating helpful incentives to produce semiconductors (CHIPS) for America act", approvato in doppia lettura e riferito alla Commissione finanze del Senato per l'approvazione degli oneri finanziari;

l'iniziativa dell'amministratore delegato della Intel Corporation rientra pertanto nell'ambito della strategia statunitense di sicurezza nazionale e di drastica riduzione della dipendenza dalla catena di approvvigionamento dei semiconduttori dai Paesi asiatici;

in linea con gli indirizzi dell'amministrazione statunitense, a seguito della firma di una dichiarazione congiunta da parte di 22 Stati membri dell'Unione europea, inclusa l'Italia, la Commissione europea ha lanciato nel giugno 2021 l'alleanza sulle tecnologie di processori e semiconduttori finalizzata al rafforzamento delle filiere domestiche, con particolare riferimento alla capacità manifatturiera;

rilevato che:

secondo i dati della Commissione europea, nel 2018 il valore dei semiconduttori nei sistemi elettronici ha raggiunto il 31,4 per cento. Le vendite mondiali di semiconduttori sono state di 113,6 miliardi di dollari nel terzo trimestre del 2020. A livello globale, la previsione della tendenza del mercato a lungo termine per i componenti elettronici è il superamento dei 1.000 miliardi di dollari entro il 2030;

tra le 7 *flagship* della strategia annuale di crescita sostenibile del 2020, di cui alla comunicazione della Commissione COM(2019) 650 final del 17 dicembre 2019, su cui si fonda la valutazione dei piani nazionali di ripresa e resilienza, la sesta, denominata "*scale-up*", riconosce che la transizione digitale della UE dipende dall'aumento delle capacità delle infrastrutture *cloud* dell'industria europea e dalla capacità di sviluppare componentistica più performante, all'avanguardia e sostenibile, e per tale ragione individua l'obiettivo di raddoppiare la produzione di semiconduttori in Europa entro il 2025, per produrre processori 10 volte più efficienti dal punto di vista energetico e consentire la rapida diffusione delle auto connesse e il raddoppio della quota di

aziende della UE che utilizzano servizi *cloud* avanzati e *big data* dal 16 per cento di oggi;

conseguentemente, il piano nazionale di ripresa e resilienza predisposto dal Governo italiano e approvato definitivamente dal Parlamento il 27 aprile 2021 include, nella componente 2 della missione 1, lo stanziamento di 750 milioni di euro di contributi a sostegno di progetti industriali ad alto contenuto tecnologico, tra i quali ricade la produzione di semiconduttori, ripartiti tra l'investimento 1 ("transizione 4.0") e l'investimento 2 ("investimenti ad alto contenuto tecnologico");

ritenuto che:

l'eventuale collocazione dello stabilimento Intel di lavorazione di semiconduttori sul territorio nazionale rappresenterebbe una grande opportunità per la creazione di posti di lavoro di qualità, lo sviluppo territoriale, il trasferimento tecnologico e il rafforzamento delle università e dei centri di ricerca italiani;

le potenziali ripercussioni negative sui Paesi europei derivanti dalle tensioni strategiche e commerciali in atto nel mercato dei semiconduttori possono essere mitigate attraverso il rafforzamento dell'autonomia strategica europea, che consiste, in questo caso, in una quota maggiore di approvvigionamento domestico di semiconduttori, cruciali per la produzione di beni finiti indispensabili per il mantenimento di livelli elevati di qualità della vita,

impegna il Governo ad adottare, presso tutte le sedi istituzionali opportune, ogni iniziativa volta a favorire l'Italia come sede di attività di lavorazione di semiconduttori, e a prevedere semplificazioni burocratiche e incentivi adeguati per l'attrazione di investimenti stranieri e lo stabilimento sul territorio nazionale di attività produttive da parte di aziende estere, al fine di rafforzare l'autonomia strategica italiana ed europea nell'approvvigionamento di semiconduttori e garantire il mantenimento di adeguati livelli di ricerca e sviluppo in ambito tecnologico, della microelettronica e dell'intelligenza artificiale.

(1-00410)

Interpellanze

BARBARO - *Al Ministro dello sviluppo economico*. - Premesso che:

il DVB-T2 (*Digital Video Broadcasting - Second Generation Terrestrial*) è lo *standard* di ultima generazione per le trasmissioni sulla piattaforma digitale terrestre. Tutti gli utenti e le emittenti televisive dovranno adeguarsi al nuovo *standard* ed è per questo che, da mesi, è principiata una campagna di comunicazione rivolta ai telespettatori, al fine di informarli sulla necessità di acquistare TV di ultima generazione o specifici *decoder* per continuare a poter usufruire del servizio con il vecchio televisore;

il decreto ministeriale 19 giugno 2019 ha fissato al prossimo 1° settembre il cambio di codifica di tutte le trasmissioni nazionali sull'intero territorio italiano (*switch-off*), quale passaggio intermedio funzionale ad accompagnare gli utenti verso le nuove tecnologie e a consentire il riassetto delle frequenze ai fini del rilascio, entro il 30 giugno 2022, della banda 700 MHz ai servizi di radiocomunicazione di nuova generazione;

il passaggio da DVB-T (*standard* MPEG2) a DVB-T2, infatti, consente di avere un maggiore numero di canali con un minore numero di frequenze, tuttavia, a causa dei ritardi di assegnazione dell'ulteriore capacità di trasmissione disponibile in ambito nazionale, delle assegnazioni dei diritti d'uso delle frequenze agli operatori di rete nazionali e locali, il Governo ha recentemente ammesso che i ritardi accumulati non consentono di perseguire il piano originale, che prevedeva il cambio di tecnologia in due *step*: il primo a settembre 2021 e il secondo a giugno 2022. Allo stato il passaggio obbligato delle trasmissioni in DVB-T2 è posticipato al 1° gennaio 2023, tuttavia nel periodo intermedio (luglio 2022 - gennaio 2023) le emittenti dovranno organizzarsi per già trasmettere in DVB-T MPEG4, potendo contare su meno frequenze, e quindi, in concreto, rinunciare a qualche canale o ridurre la qualità della trasmissione;

l'interpellante, all'uopo, esprime il suo scetticismo sulle incertezze circa i piani di intervento necessari per coordinare il riassetto della tv digitale terrestre ai fini del rilascio della banda 700 MHz agli operatori di comunicazione entro il 30 giugno 2022, e la conseguente preoccupazione che ciò possa rendere grave nocumento sia alla informazione, sia alla tenuta finanziaria delle imprese radiotelevisive;

a ciò si aggiunga che le imprese fornitrici di apparati di ricezione si sono impegnate affrontando ingenti investimenti per mettere a disposizione degli utenti milioni di nuovi apparati in tempo utile; il solo valore della merce aggiuntiva mobilitata, e in larga parte già acquisita e in arrivo in Italia per far fronte alla transizione del 1° settembre 2021, ammonta a oltre mezzo miliardo di euro, a cui vanno aggiunti i maggiori costi non comprimibili di logistica per il trasporto e lo stoccaggio straordinario delle merci: si tratta di un impegno sostanzioso, sia per i grandi produttori globali presenti nel nostro Paese, sia per le piccole e medie imprese nazionali fornitrici di ricevitori, che in questo periodo hanno più che decuplicato la propria esposizione e sulle quali, in caso di un mancato rapido ritorno degli investimenti, graverebbe un'immediata crisi di liquidità, incompatibile con la sopravvivenza stessa delle aziende,

si chiede di conoscere:

quali siano i provvedimenti che il Ministro in indirizzo ha assunto e quali quelli che intenda assumere al fine di preservare la pluralità del servizio televisivo durante le fasi intermedie del passaggio alla nuova tecnologia;

come intenda sostenere e ristorare tutti gli operatori economici ed imprenditoriali dai danni ed i pregiudizi conseguenti e conseguenziali alla posticipazione dell'impiego della piattaforma terrestre di seconda generazione,

con particolare riferimento a quelli del comparto della produzione e della vendita dei ricevitori, enormemente esposti per adempiere alla crono-tabella prevista e che, in seguito allo slittamento dei tempi, rischiano di non poter più sopravvivere sul mercato.

(2-00089)

Interrogazioni

FEDELI, BOLDRINI, BITI, COLLINA, FERRARI, MARCUCCI, ALFIERI, ASTORRE, CERNO, COMINCINI, D'ALFONSO, FERRAZZI, GIACOBBE, IORI, LAUS, MANCA, MARGIOTTA, MARILOTTI, PINOTTI, PITTELLA, ROJC, STEFANO, VALENTE, VATTUONE, VERDUCCI - *Al Ministro della salute*. - Premesso che:

il centro studi sulla libertà di religione credo e coscienza (LIREC) segnala che alcune categorie di persone sarebbero ancora escluse dalle prenotazioni per la vaccinazione anti COVID-19. In particolare si tratterebbe di cittadini comunitari in condizione di irregolarità amministrativa, di richiedenti asilo che ancora non hanno potuto accedere al servizio pubblico, di soggetti apolidi, nonché di soggetti socialmente fragili, di senza dimora, di coloro che vivono in insediamenti informali o comunque di chi non ha un medico di base o ha difficoltà di accesso al servizio sanitario nazionale. A queste categorie si aggiungono le persone che hanno intrapreso il procedimento di regolarizzazione, tra cui *caregiver* di persone fragili, che, nonostante la circolare del Ministero della salute del 14 luglio 2020 chiarisca senza ombra di dubbio il loro diritto-dovere di iscrizione al SSN, non riescono di fatto ad iscriversi e dunque ad accedere alla registrazione telematica per il vaccino, poiché il codice fiscale provvisorio rilasciato dall'INPS, non essendo alfanumerico, non viene riconosciuto dal sistema informatico;

in particolare il LIREC segnala la sua preoccupazione per l'ordinanza n. 7/2021 del commissario straordinario per l'emergenza, che all'art. 1 fornisce disposizioni riguardo alla "somministrazione dei vaccini per la prevenzione delle infezioni da SARS-CoV-2 a individui non iscritti al Servizio Sanitario Nazionale", e, nell'elencare le categorie di soggetti ammessi, non fa riferimento ad alcuna delle categorie menzionate;

ciò rappresenta un pericolo non solo per le categorie escluse, ma anche per la comunità nel suo complesso ai fini di una lotta efficace contro la diffusione della pandemia,

si chiede di sapere se i fatti riportati corrispondano al vero e, in caso affermativo, quali iniziative il Ministro in indirizzo intenda adottare, anche con il diretto coinvolgimento delle comunità di immigrati e di mediatori culturali, per superare tali difficoltà e consentire effettivamente la vaccinazione a tutti coloro che si trovano sul territorio nazionale pur non avendo documenti

quali tessera sanitaria, documento di identità o codice fiscale, anche valutando l'opportunità di adottare iniziative normative che possano consentire ai portali telematici in uso nelle diverse Regioni la prenotazione telematica per tali soggetti, al fine di evitare che pastoie burocratiche vanifichino la necessità di dare urgente risposta a un'istanza di salute pubblica globale.

(3-02769)

FREGOLENT - *Al Ministro della salute*. - Premesso che:

nel novembre 2020, un *team* di ricerca dell'università Statale di Milano ha sviluppato un *test* salivare molecolare per COVID-19, basato e ottimizzato su un protocollo dell'università di Yale, disponibile in *open science*;

esso è autosomministrabile, senza necessità di personale per il prelievo, il che lo rende assai adatto per la sorveglianza attiva e consente una notevole riduzione dell'impiego di personale sanitario, da impiegare per esempio nella campagna di vaccinazione;

il Ministero della salute, con la circolare n. 21675 del 14 maggio 2021, ha fornito chiarimenti sull'impiego dei *test* salivari per la diagnosi di infezione da SARS-CoV-2, stabilendo che per rilevare un'infezione da coronavirus si possono usare anche i *test* salivari, nel momento in cui non sia possibile avere a disposizione tamponi oro-nasofaringei e preferibilmente per "screening ripetuti" per motivi professionali o di altro tipo, sugli anziani o disabili e sui bambini in ambito scolastico;

i tamponi salivari sono stati sperimentati con successo in diverse realtà del nostro Paese e la loro attendibilità è sensibilmente migliorata rispetto al passato. Si tratta di un *test* ideale soprattutto per i più piccoli, che potrebbero risentire dell'eccessiva invasività dei tamponi molecolari classici. Alcuni studi pubblicati nel 2020 hanno rilevato sensibilità comprese tra il 53 e il 73 per cento e un'attendibilità che può arrivare fino al 98 per cento, come dimostrato durante l'utilizzo nelle scuole della Lombardia da maggio;

nella scelta di sottoporre i bambini al vaccino è necessario valutare puntualmente il rapporto tra rischi e benefici, dal momento che il rischio dei bambini con buone condizioni di salute di ammalarsi è bassissimo, e nessuno conosce gli effetti a medio e lungo termine dei vaccini anti COVID, somministrati per la prima volta. Peraltro il meccanismo dell'mRna (quello che riguarda Pfizer e Moderna) non è mai stato usato prima nei vaccini, e quindi si è dinanzi a un inedito assoluto;

l'effettuazione del vaccino non annienta il rischio di contagiarsi, considerato che i vaccini danno una protezione che va dal 60 al 90 per cento, dunque anche un soggetto vaccinato può essere portatore del virus, e quindi al fine di scongiurare il propagarsi del virus devono essere effettuati comunque dei controlli frequenti;

per i più giovani il principio di massima precauzione imporrebbe di prevedere che si individui la soluzione che comporti i maggiori benefici al

minor rischio, e un sistema basato sul tracciamento continuo come quello garantito dai tamponi salivari, che assicurano al contempo un'alta attendibilità coniugata a una bassa invasività del trattamento, risulta essere la migliore soluzione;

le ultime rilevazioni dell'INVALSI sull'apprendimento scolastico, quale emerge dai *test* effettuati quest'anno *on line*, testimoniano il sostanziale fallimento della didattica a distanza (DAD) nel primo anno di applicazione ed accentuano l'urgenza di porre un argine alle disfunzioni della scuola. Facendo emergere, così, chiaramente che tra le vittime più importanti della pandemia vanno purtroppo annoverati l'istruzione e l'apprendimento dei giovani;

la presente tematica sottende due diritti fondamentali e irrinunciabili, da un lato il diritto alla salute e dall'altro il diritto all'istruzione. Tale contrapposizione impone che sia trovata la soluzione più soddisfacente per la garanzia contestuale di questi due diritti di pari rango costituzionale,

si chiede di sapere se il Ministro in indirizzo, secondo le modalità individuate nella propria circolare del 14 maggio 2021, non ritenga doveroso e urgente adottare un protocollo unico nazionale, da applicare presso gli istituti scolastici di ogni ordine e grado, volto a prevedere l'effettuazione di *test* salivari, affinché sia assicurato il ritorno in presenza nelle scuole in vista della partenza del nuovo anno scolastico a settembre, scongiurando il ritorno alla didattica a distanza.

(3-02770)

BERGESIO, VALLARDI, RUFA, ZULIANI - *Al Ministro delle politiche agricole alimentari e forestali*. - Premesso che:

la "NotCo", *start-up* specializzata nella produzione di alimenti con ingredienti vegetali, ha chiuso con un aumento di capitale di 235 milioni di dollari, sottoscritto da investitori di rilievo internazionale;

l'aumento di capitale risulta infatti sottoscritto da un fondo di *venture capital* "Tiger Global", affiancato fra gli altri anche da "Bezos Expeditions", *family office* del fondatore di "Amazon" e da "L Catterton", *private equity*, controllato da "Lvmh" e dalla famiglia Arnault;

dal fondo di *venture capital*, la *start-up* ha ottenuto capitali per circa 350 milioni di dollari per sviluppare cibi vegani in tutto simili agli originali, come latte, uova e carne; per lo scopo la società ha creato un algoritmo che esplora più combinazioni di ingredienti vegetali per replicare i sapori degli alimenti tradizionali;

quello dei cibi sintetici è un mercato in forte espansione; secondo una ricerca di Boston consulting group e Blue Horizon, il suo giro di affari potrebbe toccare i 290 miliardi di dollari entro il 2035, tanto da attirare gli investimenti da parte di celebrità dello sport, del cinema e della musica, che hanno fornito anche un'importante spinta pubblicitaria alle aziende che operano nel settore;

si sta generando un'agguerrita concorrenza che indebolisce la competitività dell'agroalimentare italiano, le cui eccellenze rischiano di essere travolte nel livellamento creato dalla globalizzazione, la quale sostiene la diffusione di modelli alimentari, assolutamente lontani dalla nostra cultura e dalle nostre tradizioni, basati sulla promozione di cibi ultra processati e sintetici, non adatti a garantire il giusto apporto nutrizionale nella dieta alimentare;

le filiere zootecniche, già sfiancate dal calo della domanda per effetto della pandemia da COVID-19, sono in stato di forte allarme e preoccupazione, anche alla luce del dibattito che sta nascendo intorno a queste nuove frontiere del cibo, di cui ormai parlano tutti gli organi di informazione;

la filiera agroalimentare, dai campi alla tavola, vale oggi il 25 per cento del PIL e garantisce lavoro a 3,8 milioni di persone, grazie all'attività, tra gli altri, di 740.000 aziende agricole, 70.000 industrie alimentari, oltre 330.000 realtà della ristorazione e 230.000 punti vendita al dettaglio; è necessario mettere in atto tutti gli sforzi possibili per tutelare questo importante patrimonio, espressione di tradizioni, esperienze e specificità territoriali,

si chiede di sapere se il Ministro in indirizzo, alla luce delle risorse messe a disposizione dal PNRR e dal piano di investimenti della nuova PAC, voglia indicare gli interventi necessari ad incentivare la diffusione di modelli alimentari che, basati sul principio della dieta mediterranea, offrano garanzia di qualità e salubrità degli alimenti, tenendo conto anche della centralità del sistema agroalimentare *made in Italy* per l'economia del Paese.

(3-02771)

CALANDRINI - *Ai Ministri del lavoro e delle politiche sociali e dello sviluppo economico*. - Premesso che:

l'azienda Corden Pharma Latina S.p.A., con stabilimento sito presso Sermoneta (Latina), ha avviato in data 9 novembre 2018 una procedura di licenziamento collettivo per riduzione del personale nei confronti di 192 lavoratori, divenuti successivamente 188 per risoluzioni interne;

tale procedura è stata conclusa, a seguito dell'esame congiunto *ex* legge n. 223 del 1991, mediante un accordo tra le parti sociali, l'azienda e la Regione Lazio, Direzione generale del lavoro, Area vertenze ed interventi, con un accordo siglato il 17 gennaio 2019 da tutti i presenti, che impegnava l'azienda a proseguire nel piano di investimenti per 35 milioni di euro nell'arco di 4 anni (2020-2023) su nuove linee di produzione per la preparazione di prodotti oncologici ed antibiotici;

le parti sociali davano il loro assenso per la riduzione del costo del lavoro, per l'esodo di lavoratori in possesso dei requisiti per usufruire degli scivoli in uscita dal lavoro attivo, il ricorso all'intervento straordinario di integrazione salariale per crisi aziendale, l'esternalizzazione di servizi con relativa riassunzione di almeno 35 figure, la cessione di contratti di lavoro a società del gruppo e con l'agevolazione a ricorrere a strumenti, quali l'accordo collettivo di incentivazione e il contratto di sviluppo;

tale accordo è stato sostenuto presso il Ministero dello sviluppo economico (struttura per la crisi di impresa) nel successivo 21 gennaio 2019, confermando che gli investimenti ed i sostegni a quanto concordato fossero subordinati al mantenimento dei livelli occupazionali nell'azienda;

il 26 luglio 2021 l'azienda, disattendendo tali accordi, ha provveduto ad informare le stesse parti sociali che avrebbe dato corso alla procedura di licenziamento per 120 persone;

il 29 luglio l'azienda Corden Pharma Latina ha comunicato alle organizzazioni sindacali, ai sensi della legge n. 223 del 1991, l'avvio della procedura di licenziamento collettivo per 82 dipendenti;

appare evidente che l'azienda non sembra interessata a concorrere ad usufruire dei fondi di investimento pubblici, come asserito nell'accordo del 17 gennaio 2019;

anche la cessione del ramo d'azienda prevista nell'accordo dalla piattaforma ecologica Ecoplataform ad Itelyum, facenti parte del medesimo gruppo, non è mai stata perfezionata;

la manovra rischia di essere finalizzata alla dismissione di unità produttive che comporterà la dispersione di professionalità e del tessuto produttivo nel comparto industriale del settore farmaceutico, che è patrimonio del territorio pontino e nazionale;

per i lavoratori di Corden Pharma non solo si prospetta un'incognita rispetto al proprio futuro, ma è forte anche il rischio di non poter usufruire degli ammortizzatori sociali previsti dal Governo con il decreto del 1° luglio 2021;

a parere dell'interrogante la provincia di Latina non può permettersi un'altra crisi occupazionale, in particolare nel settore farmaceutico, che è uno dei più importanti in termini di PIL ed esportazioni per il territorio locale, nonché un polo di riferimento in ambito nazionale,

si chiede di sapere:

come i Ministri in indirizzo intendano procedere affinché venga dato seguito all'accordo siglato il 17 gennaio 2019, dalle parti sociali, con la Regione Lazio, Direzione generale del lavoro, Area vertenze ed interventi, e l'azienda, che impegnava quest'ultima a proseguire nel piano di investimenti per 35 milioni di euro nell'arco di 4 anni (2020-2023) su nuove linee di produzione per la preparazione di prodotti oncologici ed antibiotici;

se non intendano intervenire al fine comunque di pervenire ad una soluzione che eviti la perdita dei posti di lavoro, consenta eventualmente l'applicazione degli ammortizzatori sociali e garantisca continuità ai lavoratori, ponendo in essere tutte le azioni necessarie per non disperdere un patrimonio produttivo di grande rilievo per il tessuto economico pontino e per il settore farmaceutico nazionale.

(3-02772)

BOLDRINI - *Al Ministro della salute*. - Premesso che:

in Italia 5 milioni di persone soffrono di incontinenza e il 60 per cento sono donne;

tale patologia è ancora vissuta come un vero stigma sociale, e in tale ottica il Ministero della salute, con direttiva del Presidente del Consiglio dei ministri 10 maggio 2006, ha indetto il 28 giugno la "giornata nazionale per la prevenzione e la cura dell'incontinenza";

la giornata è stata promossa dai pazienti e voluta dal Ministero della salute e ha le seguenti finalità: "Nell'ambito di tale giornata, le amministrazioni pubbliche e gli organismi di volontariato s'impegnano a promuovere, attraverso idonee iniziative di sensibilizzazione e solidarietà, quali il contributo di specialisti, che effettueranno controlli medici gratuitamente, l'attenzione e l'informazione sui problemi delle persone incontinenti e di quanti sono coinvolti, direttamente o indirettamente, nelle loro vicende, al fine di sviluppare politiche pubbliche e private che allarghino le possibilità di guarire dalla malattia, o quantomeno conviverci con dignità";

in Italia l'incontinenza incide pesantemente sulla qualità e quantità di vita provocando nelle persone colpite isolamento sociale, ansia e depressione che fanno sì che solo una piccola minoranza si rivolga al medico di famiglia. La patologia, invece, come evidenziano i massimi esperti nel settore, nella stragrande maggioranza dei casi può essere curata con successo tramite la rieducazione perineale, la chirurgia mininvasiva, la neuromodulazione e altre terapie;

stime indicano che lo Stato, tramite Regioni e ASL, spende oltre 420 milioni di euro all'anno (più IVA al 4 per cento e costi della filiera) per i soli pannoloni, mentre tramite l'implementazione di percorsi riabilitativi i costi si ridurrebbero drasticamente. I costi globali del settore, tra pubblico e privato sociale, ammontano a circa 2,5 miliardi di euro annui, come stima l'associazione dei pazienti Fincopp (Federazione italiana incontinenti e disfunzioni del pavimento pelvico);

l'incontinenza è, come detto, un vero e proprio tabù medico ed è pertanto importante divulgare le problematiche e le possibili soluzioni. A tal proposito, sarebbe fondamentale attivare appositi "centri";

un tavolo sull'incontinenza è stato istituito nel 2015 (decreto ministeriale 2 ottobre 2015) dal Ministro della salute *pro tempore* e ha prodotto l'accordo della Conferenza Stato-Regioni del 24 gennaio 2018, che prevede l'attivazione dei tavoli di lavoro regionali sull'incontinenza e l'apertura dei centri di primo, secondo e terzo livello in ogni regione;

l'accordo prevede infatti che in ogni Regione venga istituita una rete regionale di centri per la prevenzione, diagnosi e cura dell'incontinenza articolata su tre livelli, prevedendo inoltre che quelle che non hanno realizzato la rete dei centri provvedano a costituire un apposito gruppo di lavoro locale,

propedeutico alla realizzazione della rete regionale, nel quale trovino adeguata rappresentatività le competenze cliniche ed organizzative delle amministrazioni regionali oltre che di esperti di settore;

ad eccezione di Piemonte e Veneto, nelle altre Regioni non si ha notizia dell'attuazione dell'accordo;

proprio per monitorare l'operatività delle regioni e l'attivazione dei tavoli regionali con l'apertura dei centri riabilitativi, a parere dell'interrogante, sarebbe utile ed indispensabile attivare presso il Ministero della salute un tavolo permanente e ristretto sull'incontinenza urinaria, fecale e disturbi al pavimento pelvico, con la partecipazione delle associazioni pazienti;

il tavolo non comporta per il Ministero alcun onere economico, poiché le riunioni possono svolgersi da remoto e con oneri economici a carico dei partecipanti,

si chiede di sapere quale sia lo stato dell'arte relativo all'attuazione ed implementazione dell'accordo della Conferenza Stato-Regioni del 24 gennaio 2018 e se non ritenga urgente intraprendere immediate iniziative al fine di attivare il suddetto tavolo ministeriale.

(3-02775)

LA MURA - *Al Ministro della transizione ecologica*. - Premesso che:

la rete "Natura 2000" è il principale strumento della politica della UE per la conservazione della biodiversità. Si tratta di una rete ecologica, istituita ai sensi della direttiva 92/43/CEE "Habitat" per garantire il mantenimento a lungo termine degli *habitat* naturali e delle specie di flora e fauna minacciati o rari a livello comunitario;

essa comprende i siti di interesse comunitario (SIC), identificati dagli Stati membri secondo quanto stabilito dalla direttiva Habitat, che vengono successivamente designati quali zone speciali di conservazione (ZSC), e anche le zone di protezione speciale (ZPS), istituite ai sensi della direttiva 2009/147/CE "Uccelli";

in data 9 giugno 2021 la UE ha avviato nei confronti dell'Italia la procedura di infrazione n. 2021/2028 sul mancato completamento della designazione dei siti della rete Natura 2000;

più nel dettaglio, secondo la Commissione europea, allo stato attuale la rete Natura 2000 dell'Italia non comprende nella misura adeguata tutti i diversi tipi di *habitat* e le specie che necessitano di protezione. Le lacune più gravi riguardano le specie marine, come la foca monaca mediterranea, la tartaruga marina comune e il tursiope, e gli *habitat* marini, come le scogliere. Mancano, inoltre, le designazioni dei siti marini per diverse specie di uccelli marini, come la berta maggiore e la berta minore;

il nostro Paese dispone di due mesi per rispondere alla lettera di messa in mora e adottare le misure necessarie, al fine di evitare che la Commissione possa adottare un parere motivato,

si chiede di sapere:

se il Ministro in indirizzo sia a conoscenza dei fatti esposti e di altri elementi al riguardo;

se intenda adottare le misure necessarie per l'immediata chiusura della procedura di infrazione, scongiurando così che essa possa proseguire con l'emissione di un parere motivato da parte della Commissione europea.

(3-02777)

LA MURA - *Al Ministro della transizione ecologica*. - Premesso che:

anche quest'anno l'interrogante ha lanciato, attraverso i propri canali *social*, una campagna per ricevere segnalazioni dai cittadini su problematiche relative al mare e alle spiagge dagli stessi frequentate nella stagione estiva;

a seguito di tale iniziativa, la presente firmataria ha ricevuto numerose segnalazioni, supportate da consistente documentazione fotografica, che denunciano una situazione di degrado e di inquinamento davvero allarmante relativa al Rivo d'Arco, alla sua foce presso la Marina di Seiano e alla spiaggia, ricadenti nel territorio del Comune di Vico Equense;

più nel dettaglio, secondo le segnalazioni, il Rivo d'Arco è gravemente inquinato e maleodorante, contiene scarichi illeciti, materiali di risulta, e molto probabilmente anche liquami fognari, residui della lavorazione lattiero casearia e rifiuti edili. Questa situazione di inquinamento si ripercuote sulla foce del Rivo presso la Marina di Seiano e sulla spiaggia;

le acque del Rivo d'Arco, anche per effetto di poche ore di pioggia, trasportano i materiali inquinanti in mare, rendendo le acque marroni, e sulla spiaggia, trasformandola in una fogna a cielo aperto;

l'area in oggetto è un sito di importanza comunitaria (SIC) e al contempo una zona di protezione speciale (ZPS);

il Comune di Vico Equense ospita cinque spiagge "Bandiera Blu" della FEE (Fondazione per l'Educazione Ambientale), tra le quali vi è anche quella di Marina di Seiano Ovest Porto. A parere dell'interrogante, è inaccettabile, in primo luogo, che esistano ancora situazioni di inquinamento come quelle del Rivo d'Arco, e, in secondo luogo, che tale situazione riguardi un territorio con riconoscimenti internazionali come la Bandiera Blu;

in data 30 luglio 2021 l'interrogante ha segnalato i fatti esposti al Comune di Vico Equense, alla Regione Campania, alla FEE, alla Guardia costiera e alla Capitaneria di Porto competenti per territorio, al fine di sollecitare azioni immediate di verifica, monitoraggio, controllo e risoluzione dei problemi descritti;

considerato che:

la Strategia dell'UE sulla biodiversità entro il 2030 ha evidenziato il nesso esistente tra lo stato di degrado degli ecosistemi naturali, compresi quelli fluviali e marini, e la comparsa e la diffusione di malattie: la salute

dell'uomo dipende dalla salute della natura. Sono, pertanto, necessarie azioni di conservazione degli ecosistemi naturali e di ripristino di quelli degradati;

in data 12 maggio 2021 la Commissione UE ha adottato la comunicazione "Un percorso verso un pianeta più sano per tutti Piano d'azione dell"UE: "Verso l'inquinamento zero per l'aria, l'acqua e il suolo" (COM(2021) 400), secondo la quale entro il 2050 ??L'inquinamento dell'aria, dell'acqua e del suolo è ridotto a livelli che non sono più considerati nocivi per la salute e per gli ecosistemi naturali e che rispettano limiti sostenibili per il nostro pianeta, così da creare un ambiente privo di sostanze tossiche??;

occorre intervenire con tempestività al fine di rimuovere le cause di inquinamento per arrestare il degrado degli ecosistemi naturali, tutelare la salute dei cittadini, e al contempo assicurare lo sviluppo sostenibile dei territori attualmente interessati da fenomeni di inquinamento,

si chiede di sapere se il Ministro in indirizzo sia a conoscenza dei fatti esposti o di altri elementi al riguardo, e quali iniziative intenda adottare al fine di rimuovere la situazione di inquinamento del Rivo d'Arco, ripristinare gli ecosistemi naturali degradati per effetto dello stesso, e, più in generale, quali azioni intenda intraprendere per porre rimedio a situazioni di inquinamento analoghe a quella descritta, presenti sul nostro territorio.

(3-02778)

LA MURA - *Ai Ministri delle infrastrutture e della mobilità sostenibili e della transizione ecologica*. - Premesso che:

il 23 luglio 2014 la UE ha approvato la direttiva 2014/89/UE, che istituisce un quadro per la pianificazione dello spazio marittimo, in forza della quale gli Stati membri sono tenuti provvedere alla pianificazione degli spazi marittimi e alla gestione integrata delle zone costiere, secondo un approccio ecosistemico;

più nel dettaglio, gli Stati devono pianificare e regolare gli usi diversi dello spazio marittimo, limitando i conflitti e creando opportune sinergie. L'elaborazione dei piani di gestione per l'attuazione della pianificazione marittima è fondamentale per individuare la distribuzione spaziale e temporale delle pertinenti attività e dei pertinenti usi delle acque marine, presenti e futuri, che possono includere: aree per la produzione dell'acquacoltura, aree dove è consentita la pesca, aree per la produzione di energia da fonti rinnovabili, rotte di trasporto marittimo e flussi di traffico, ivi compreso il sistema portuale, zone di addestramento militare, siti di conservazione della natura e di specie naturali e zone protette, zone di estrazione di materie prime, ricerca scientifica, tracciati per cavi e condutture sottomarine, turismo, patrimonio culturale sottomarino, paesaggi costieri;

secondo la direttiva, la pianificazione deve fondarsi su un approccio ecosistemico, definito dalla direttiva quadro sulla strategia per l'ambiente marino (direttiva 2008/56/CE) come segue: "una strategia che promuove la conservazione e un uso sostenibile ed equo del suolo, dell'acqua e delle risorse

viventi attraverso una gestione integrata degli stessi. L'obiettivo della gestione ecosistemica è di mantenere un ecosistema in una condizione sana, produttiva e resiliente affinché possa fornire agli esseri umani i beni e i servizi che desiderano e di cui hanno bisogno. A differenza degli approcci attuali, solitamente mirati a una singola specie, attività, settore o problema, la gestione ecosistemica considera gli impatti cumulativi di diversi settori";

la direttiva, che stabilisce come termine ultimo per l'adozione dei piani di gestione dello spazio marittimo, da parte degli Stati membri, il 31 marzo 2021, è stata recepita in Italia con il decreto legislativo 17 ottobre 2016, n. 201, che individua il Ministero delle infrastrutture e della mobilità sostenibili quale autorità competente per la sua attuazione;

con decreto del Presidente del Consiglio dei ministri 1° dicembre 2017 sono state approvate le linee guida contenenti gli indirizzi e i criteri per la predisposizione dei piani di gestione dello spazio marittimo. Esse sottolineano la necessità di garantire la coerenza tra i piani marittimi e gli obiettivi della direttiva quadro sulla strategia per l'ambiente marino;

l'art. 5 del decreto legislativo prevedeva originariamente come termine ultimo per l'adozione dei piani il 31 dicembre 2020. Tale termine è stato posticipato al 31 marzo 2021, in forza dell'art. 13, comma 5-*bis*, del decreto-legge 30 dicembre 2019, n. 16;

ad oggi non è stata ancora avviata la procedura di valutazione ambientale strategica (VAS) in relazione ai citati piani;

considerato che:

in data 1° febbraio 2021 è stata avviata la procedura di VAS del piano per la transizione energetica sostenibile delle aree idonee (PiTESAI), che attualmente è nella fase della consultazione pubblica. Il piano, introdotto dall'art. 11-*ter* del decreto-legge 14 dicembre 2018, n. 35, è diretto ad individuare le aree dove sarà possibile svolgere o continuare a svolgere le attività di ricerca, prospezione e coltivazione degli idrocarburi in modo sostenibile;

il piano si occuperà delle attività di prospezione, ricerca e coltivazione di idrocarburi a terra e in mare. Quindi, per quanto attiene alle attività in mare, si configura un'interferenza con la pianificazione spaziale marittima, che, come anticipato, si riferisce a tutti gli usi del mare;

tenuto conto dello stato della procedura di VAS del piano per la transizione energetica sostenibile delle aree idonee, questo sarà approvato prima dell'approvazione dei piani di gestione dello spazio marittimo, con conseguente individuazione delle aree idonee e delle aree non idonee all'attività mineraria, senza tener conto della preliminare definizione e composizione di tutti gli altri usi del mare;

la pianificazione spaziale marittima è uno strumento di primo livello, sovraordinato, cioè, agli ulteriori e previgenti atti di pianificazione della gestione del "territorio marino", il cui contenuto deve necessariamente confluirvi. Più precisamente, essa rientra nella tipologia dei "superpiani";

in data 14 maggio 2021, con parere n. 14, la commissione tecnica di verifica dell'impatto ambientale ha raccomandato "ai fini della massima coerenza tra PiTESAI e la Pianificazione dello Spazio Marittimo, di tener conto di quanto in corso di redazione da parte del Gruppo di lavoro istituito all'interno del Comitato Tecnico per la Pianificazione dello Spazio Marittimo, in cui siedono rappresentanti del Ministero delle Infrastrutture e delle Mobilità sostenibili (MIMS) e del MiTE";

nella proposta di piano del 15 luglio 2021 si precisa, in relazione ai rapporti tra lo stesso e la pianificazione spaziale marittima, quanto segue: "Attualmente la MSP, in Italia, è tuttavia in fase di redazione e non è ancora disponibile la versione definitiva della stessa, per come consolidata a valle del processo di VAS. Si ritiene, quindi, che la MSP dovrà considerare quanto prodotto sinora dal presente Piano, che potrà essere comunque oggetto di opportune future verifiche e armonizzazioni ulteriori con la MSP, nel caso di un aggiornamento del PiTESAI (per esempio con frequenza triennale)",

si chiede di sapere:

se i Ministri in indirizzo siano a conoscenza dei fatti esposti o di altri elementi al riguardo;

se, nei limiti delle rispettive competenze, intendano chiarire le cause del ritardo nell'approvazione dei piani di gestione dello spazio marittimo, nonché precisare quando ritengono, almeno in via approssimativa, che tali piani saranno approvati;

se, sempre nei limiti delle rispettive competenze, intendano precisare in che termini la pianificazione spaziale marittima dovrà considerare quanto previsto dal piano per la transizione energetica sostenibile delle aree idonee, atteso che la prima rientra nella categoria dei "superpiani" e l'altro costituisce un piano settoriale.

(3-02779)

CASTELLONE - *Ai Ministri delle politiche agricole alimentari e forestali e della salute*. - Premesso che:

la bufala mediterranea italiana è tutelata dalla legge 27 dicembre 2002, n. 292, che all'art.1, comma 1, recita: "La bufala mediterranea italiana è da considerare patrimonio zootecnico nazionale, le cui caratteristiche genetiche sono da tutelare dall'immissione incontrollata di capi esteri per salvaguardare le peculiari caratteristiche di tale razza; tale patrimonio deve essere tutelato altresì da tutte le patologie infettive ed infestive, mediante piani regionali di profilassi appositamente dedicati alla prevenzione ed eradicazione delle malattie a carattere diffusivo, a salvaguardia delle produzioni di filiera e del consumatore". La produzione di mozzarella di bufala DOP ha un impatto notevole sul prodotto interno lordo della Regione Campania e presenta un *trend* in forte crescita su tutti i mercati nazionali e internazionali;

l'intera filiera bufalina è regolamentata da un rigoroso disciplinare di produzione della denominazione di origine protetta (regolamento (CE) n. 1107/96, decreto ministeriale 18 settembre 2003) e determina un giro di affari di 1.218 milioni di euro annui (fonte: SVIMEZ 2019);

il comparto bufalino casertano rappresenta il 60 per cento dell'allevamento in Italia, con un impegno occupazionale diretto di oltre 40.000 addetti oltre all'indotto, tanto che lo studio SVIMEZ sull'impatto socio-economico della filiera bufalina presentato alla Borsa di Milano il 20 giugno 2019 ha concluso che "la Mozzarella di Bufala Campana Dop corre alla stessa velocità di un brand premium del settore automobilistico, generando un giro di affari di 1 miliardo e 218 milioni di euro";

tale comparto vive una fortissima difficoltà per l'imperversare della brucellosi, il cui tasso di infezione e propagazione è estremamente preoccupante, raggiungendo un valore di circa il 10 per cento portando, dal 2018 ad oggi, all'abbattimento di circa 33.000 capi di bufala mediterranea sospetti d'infezione all'esito degli esami di laboratorio eseguiti dall'Istituto zooprofilattico del Mezzogiorno che, insieme agli uffici della Regione Campania e della ASL Caserta, non consente la presenza di tecnici e periti di parte nominati dagli allevatori che vogliono verificare l'esattezza delle analisi e delle procedure adottate, come ben descritto dalla recente inchiesta giornalistica "Bufale connection" di "Fanpage";

considerato che:

fino al 2014, quando era concesso agli allevatori di poter vaccinare i capi, l'incidenza della malattia era scesa ai minimi storici raggiungendo soglie vicine all'1 per cento degli animali; tale facoltà è poi stata cancellata, permettendo solo gli abbattimenti, e la curva dei contagi ha ripreso a crescere;

nel 2019 la Regione Campania ha varato la delibera n. 207, che non consente l'applicazione del regolamento (CE) n. 1226/2002, che prevede uno specifico accertamento suppletivo con l'uso del "*test* IDT Aviare" per scongiurare l'abbattimento di falsi positivi al "*test* dell'IDT bovis", ma utilizza il *kit* diagnostico "Bovigam", che non solo non è validato-registrato per l'uso nel bufalo mediterraneo, ma non è neanche previsto dal manuale delle prove diagnostiche dell'Organizzazione mondiale della sanità animale (OIE);

gli Stati membri avrebbero dovuto adottare il regolamento (UE) 2020/689 del 17 dicembre 2019, che usa il criterio degli abbattimenti selettivi e mirati e l'avvio di un piano vaccinale per la brucellosi e altre malattie come la tubercolosi, entro il mese di aprile 2021;

rilevato che:

gli allevatori della provincia di Caserta e tutti gli operatori del settore chiedono di rivedere urgentemente il piano regionale di eradicazione della brucellosi, che finora ha dato risultati scadenti, in particolare essi invocano controlli più stringenti e puntuali per rendere realmente efficace la profilassi primaria, al fine di evitare o ridurre al minimo l'abbattimento dei capi di bestiame;

l'inserimento dell'uso dei vaccini sarebbe determinante non solo per salvare le bufale, ma anche per conservare un patrimonio genetico di alto valore, che vuol dire preservare l'economia locale fortemente identitaria;

i sindaci dei comuni casertani, nell'audizione del 10 aprile 2019 presso la 9a Commissione permanente (Agricoltura e produzione agroalimentare) del Senato, hanno richiesto l'intervento urgente degli alti livelli istituzionali nazionali e regionali affinché vengano previste immediatamente nuove e specifiche misure e procedure diagnostiche per i bufali, al fine di scongiurare i falsi positivi e l'abbattimento di bufali sani, altresì proteggendo il bestiame dall'infezione, riattivando la profilassi vaccinale contro la brucellosi dei bufali già autorizzata dalla UE, dal Ministero e dalla Regione Campania e regolarmente effettuata su base volontaria fin dall'anno 2008 a tutto il 2013;

la risoluzione approvata all'unanimità dalla 9a Commissione permanente del Senato sull'affare assegnato n. 237 (Doc. XXIV, n. 24) ha impegnato il Governo, tra i vari punti, a valutare la possibilità di istituire un tavolo con il coinvolgimento di Ministero delle politiche agricole, Ambiente e Regione Campania, per favorire e rafforzare il risanamento e lo sviluppo della filiera bufalina nelle diverse criticità; a valutare interventi a favore dell'applicazione delle misure di biosicurezza nelle aziende in cui sono state diagnosticate brucellosi o tubercolosi; a rafforzare la selezione genetica della bufala di razza mediterranea italiana che rappresenta un volano per la crescita del settore, anche puntando a lavorare per una più puntuale definizione per la popolazione bufalina e utile alla salvaguardia del patrimonio nazionale, attraverso iniziative oggetto di finanziamento nei pagamenti accoppiati, di cui all'art. 52 del regolamento (UE) n. 1307/2013 della nuova programmazione PAC e PSR,

si chiede di sapere:

se i Ministri in indirizzo siano a conoscenza della grave situazione epidemiologica che investe gli allevamenti di bufale nella provincia di Caserta e quali misure intendano intraprendere al fine di evitare la propagazione della brucellosi bufalina in Campania;

se e quando intendano porre in essere misure volte a evitare abbattimenti indiscriminati di bufala mediterranea italiana nella provincia di Caserta, considerato che le attività di verifica e profilassi per brucellosi e tubercolosi (stabilite dalla Regione Campania con la delibera n. 207 del 25 maggio 2019) danno luogo a falsi positivi e non seguono le procedure previste dal regolamento (CE) n. 1226/2002, dal regolamento (UE) n. 2016/429, dal regolamento (CE) n. 852/2004 e dall'OIE per i bufali italiani, tanto più che per la tubercolosi non viene effettuata la diagnosi differenziale con il *test* IDT Aviare, nonostante negli allevamenti siano presenti numerosi uccelli portatori di TBC aviaria non nociva per il bestiame e l'uomo, e se intendano intervenire per garantire l'uso dei vaccini contro la brucellosi (da utilizzare nelle province a rischio e su base volontaria da parte degli allevatori);

se, nei limiti delle loro competenze, e di concerto con la Regione Campania, prevedano di fornire contributi di sostegno agli allevatori che hanno subito perdite per l'abbattimento di capi poi risultati sani.

(3-02780)

DE BERTOLDI, GARNERO SANTANCHÈ, LA PIETRA, MALAN, RAUTI, TOTARO - *Ai Ministri dell'interno e della giustizia*. - Premesso che:

l'ennesima manifestazione di protesta, avvenuta il 31 luglio 2021, contro le forze dell'ordine e i militari schierati a protezione del cantiere in Valle di Susa, da parte degli anarchici di sinistra dell'area antagonista, per contestare la realizzazione della linea ferroviaria alta velocità Torino - Lione, dimostra in modo evidente, come a distanza di anni, la situazione sia divenuta oramai intollerabile;

i due agenti di Polizia feriti e gli automezzi delle forze dell'ordine pesantemente danneggiati (addirittura è stato messo fuori uso un "Lince" dell'Esercito italiano) dimostrano l'estrema violenza, determinata da azioni di guerriglia pre-organizzata (attraverso l'uso di lancia razzi, bombe carta e persino l'utilizzo di *bazooka* artigianali per lanciare ordigni incendiari contro le forze di Polizia) da parte di questo movimento anarco-eversivo di sinistra che (con il chiaro intento di uccidere o di ferire gravemente gli agenti di pubblica sicurezza) non può continuare ad essere affrontato con superficialità o disattenzione da parte del Governo e della magistratura;

i gravissimi episodi accaduti nel cantiere nella Valle di Susa evidenziano inoltre la necessità di ribadire che le regole d'ingaggio molto limitative previste dall'attuale normativa, penalizzano fortemente le forze dell'ordine, considerate a giudizio degli interroganti, vittime passive di un sistema che tutela esclusivamente i manifestanti, rendendo di fatto inerti gli agenti di pubblica sicurezza, chiamati a tutelare l'ordine pubblico e fare rispettare l'ordinamento;

al riguardo, a parere degli interroganti, risulta urgente e necessario introdurre nuove regole, stabilendo (oltre a misure volte a tutelare maggiormente le forze dell'ordine in caso d'ingaggio) tra le proposte contrattuali, quella che riguarda la tutela legale, al fine di motivare il personale delle forze dell'ordine, che quotidianamente rischia la sua vita, considerato che, in caso di denuncia, le spese legali risultano addirittura a carico del singolo agente o carabiniere, soprattutto quando di verificano episodi come quelli esposti;

a giudizio degli interroganti, appare evidentemente inutile la decisione da parte del Ministro in indirizzo, di inviare migliaia di agenti di polizia a presidiare il cantiere della TAV, se gli stessi non ricevono adeguate tutele normative, in relazione alle regole d'ingaggio (per intervenire e disperdere o arrestare i manifestanti, responsabili di azioni di guerriglia) che risultano attualmente sfavorevoli nei loro riguardi, oltre che pericolose, considerata l'organizzazione particolarmente agguerrita di tali criminali, nell'attaccare addirittura con armi da guerra, le forze dell'ordine;

destano, altresì, sconcerto e preoccupazione, a parere degli interroganti, le difficoltà da parte dello Stato e delle istituzioni preposte, nell'assicurare alla giustizia gli autori delle aggressioni alle forze dell'ordine e processarli per direttissima, considerate le complessità attuali del quadro normativo in tal senso;

a tal fine, le citate osservazioni, secondo gli interroganti, delineano un quadro sconcertante e pericoloso, in cui emergono chiaramente le difficoltà da parte dello Stato nel non riuscire a dimostrare la sua autorevolezza e la sua autorità, né tantomeno a rendere impossibile ogni forma di violenza pubblica, con le forze dell'ordine che invece sono costrette a subire ogni tipo di violenza e attacchi da parte degli anarchici insurrezionalisti, studiati nei modi e nei tempi, considerato che tali incidenti avvengono sempre a ridosso della stagione turistica, in modo da tenere lontano i turisti e arrecare più danni possibili all'economia locale,

si chiede di sapere:

quali valutazioni i Ministri in indirizzo intendano esprimere, nell'ambito delle rispettive competenze, con riferimento a quanto esposto in premessa;

se non convengano che i gravissimi episodi, accaduti nella Valle di Susa, che dimostrano un livello di intolleranza inaccettabile, evidenzino, fra l'altro, anche un vuoto normativo e organizzativo da parte dello Stato, nel contrastare le azioni violente degli antagonisti ribelli, le cui finalità chiaramente di eversione dell'ordine democratico, sono volte non solo a danneggiare una infrastruttura strategica per tutto il Paese, ma anche a creare le condizioni per una degenerazione dell'ordine pubblico;

quali misure urgenti e necessarie di competenza intendano infine assumere, al fine di rivedere le strategie, tutelando maggiormente le forze dell'ordine, dall'*escalation* da parte degli estremisti di sinistra no-TAV (che sembra divenuta inarrestabile) dopo gli ennesimi scontri in Valle di Susa, non soltanto attraverso misure volte a rafforzare il presidio del cantiere, ma attraverso interventi sanzionatori di tipo penale, più efficaci e rigorosi nei riguardi dei colpevoli di azioni criminali nei confronti delle forze di Polizia, Carabinieri e dell'Esercito, che stanno pagando un prezzo altissimo.

(3-02781)

LA PIETRA, CALANDRINI, FAZZOLARI, GARNERO SANTANCHÈ, MALAN, RAUTI, ZAFFINI - *Ai Ministri della salute e degli affari esteri e della cooperazione internazionale*. - Premesso che:

sono numerose e diffuse le segnalazioni pervenute dai nostri connazionali residenti all'estero che, in varie aree del mondo, stanno riscontrando notevoli difficoltà legate al rilascio del *green pass* e conseguentemente al rientro in Italia;

gli italiani residenti all'estero e iscritti all'AIRE risultano essere, al gennaio 2020, 5.486.081 ed è noto che al di fuori dell'area europea di farmacovigilanza sono state autorizzate ed implementate campagne vaccinali che prevedono l'inoculazione di vaccini diversi da quelli autorizzati dall'Agenzia europea del farmaco, oltre che, conseguentemente, dall'Agenzia italiana del farmaco: tra questi, il vaccino russo Sputnik e il vaccino cinese Sinopharm;

sono infatti numerosi gli italiani che, coerentemente alle disposizioni delle autorità sanitarie dei rispettivi Paesi di residenza, si sono immunizzati all'estero con i vaccini russi e cinesi, quali lo Sputnik, Sinopharm, Sinovac o altri sieri non autorizzati dalle agenzie del farmaco italiana ed europea;

tale circostanza determina allo stato attuale l'impossibilità per i nostri connazionali già immunizzati con tali vaccini di ottenere il *green pass* vaccinale, con tutte le conseguenze, gli inconvenienti e i disagi che ciò comporta in termini di limitazioni della mobilità internazionale e di necessaria osservanza dei periodi di isolamento precauzionale e quarantena fiduciaria al rientro sul territorio nazionale;

si tratta di una situazione di grave disagio che coinvolge un numero imprecisato ma presumibilmente molto elevato di nostri connazionali, residenti in Paesi che hanno fondato le campagne vaccinali sulla somministrazione di vaccini diversi da quelli autorizzati dalle autorità sanitarie europee e nazionali, e che oggi si trovano, loro malgrado, nella situazione di non vedersi rilasciato il *green pass* vaccinale pur essendo immunizzati;

pur nella consapevolezza della necessità di agire in un contesto di sicurezza generale, di contenimento dei rischi di contagio e di tutela della salute pubblica non si può comunque trascurare come la comunità scientifica internazionale non sia stata, né sia tuttora concorde nell'identificare e valutare l'efficacia dei diversi vaccini anti-COVID sviluppati e somministrati alla popolazione a livello mondiale;

analogamente, non è trascurabile, né può a parere degli interroganti divenire motivo penalizzante, né ragione di limitazione della libertà personali, la circostanza per cui i nostri connazionali residenti all'estero (peraltro, in assenza di diverse indicazioni governative o di una chiara strategia vaccinale che rendesse disponibili anche per gli italiani all'estero vaccini autorizzate dall'EMA), si trovino oggi limitati nelle possibilità di accesso e circolazione sul territorio nazionale, per il fatto di aver civilmente ottemperato alle disposizioni delle autorità sanitarie locali, trovandosi adesso nella paradossale situazione di un mancato riconoscimento dell'efficacia del siero inoculato e nell'impossibilità, d'altro canto, di immunizzarsi con sieri diversi,

si chiede di sapere quali iniziative i Ministri in indirizzo ritengano di poter adottare per consentire ai cittadini italiani residenti all'estero, già immunizzati con vaccini diversi da quelli autorizzati dall'Agenzia europea del farmaco e dall'Agenzia italiana del farmaco, anche eventualmente adottando una speciale strategia di monitoraggio delle condizioni di salute e di prevenzione idonea a garantire il contenimento dei rischi di contagio, di ottenere il rilascio del *green pass*.

(3-02783)

Interrogazioni orali con carattere d'urgenza ai sensi dell'articolo 151 del Regolamento

CONZATTI - *Al Ministro della salute*. - Premesso che:

il settore ricettivo rientra tra quelli maggiormente colpiti dalla crisi economica connessa all'emergenza da COVID-19, avendo registrato nel solo 2020 un calo di fatturato che, secondo le stime diffuse da Federalberghi, si attesta al 54,9 per cento in meno rispetto a quello dell'anno precedente, il che ha comportato, nonostante il blocco dei licenziamenti, l'abbandono del settore da parte di circa 20.000 lavoratori a tempo indeterminato;

considerando i recenti flussi turistici e quindi l'andamento dell'attuale stagione estiva, nonostante i numeri delle prenotazioni siano ancora significativamente inferiori rispetto a quelli che si registravano prima della pandemia, vi sono indicazioni di una concreta ripresa del settore, che può dipendere unicamente da un ripristino della normale attività economica;

in questa delicata fase è pertanto fondamentale tutelare la ripresa e far sì che, qualora si renda necessaria l'adozione di nuove misure di contenimento, siano sempre preferite quelle soluzioni che consentono di impedire l'aumento dei contagi, interferendo il meno possibile con lo svolgimento delle attività economiche;

sebbene il nuovo sistema di impiego delle certificazioni verdi COVID-19, di cui all'articolo 3 del decreto-legge 23 luglio 2021, n. 105, vada in questa direzione, appunto proponendosi di contenere il diffondersi della variante "delta" senza stabilire delle nuove chiusure, relativamente all'utilizzo del *green pass* nelle strutture ricettive si rileva una mancata chiarezza normativa, in quanto viene prescritto un utilizzo non uniforme dello strumento all'interno dei vari locali di cui si compongono tali strutture, il che sta già comportando la cancellazione di numerose prenotazioni, come segnalato con allarme dalle organizzazioni di settore, incluse Federalberghi e Confcommercio;

nello specifico, mentre tali strutture, in generale, sono esenti dalle nuove restrizioni, per cui resta libero l'accesso alle camere, secondo il disposto dell'articolo 3, comma 1, lo stesso articolo prevede l'utilizzo del certificato per accedere ai ristoranti, nonché alle piscine, ai centri natatori, alle palestre e ai centri benessere ubicati all'interno delle stesse strutture ricettive;

considerato che:

tali servizi costituiscono gli elementi principali dell'offerta di alcune strutture, nonché una delle principali ragioni per le quali gli ospiti possono decidere di trascorrervi una vacanza, è pacifico che si rende indispensabile fornire al più presto dei chiarimenti, al fine di permettere ad ogni ospite di

essere a conoscenza di quali attività sarà in grado di svolgere in base alla sua situazione;

per alcune categorie di soggetti che rappresentano una componente importante dei flussi turistici, come ad esempio gli italiani che hanno completato la loro vaccinazione fuori dai Paesi UE, non sono ancora note le modalità di ottenimento del *green pass*, per cui risulta ancora più urgente provvedere ad uniformare la disciplina applicabile all'interno delle strutture a quella decisa per l'accesso, che appunto non è sottoposto alla verifica del *green pass*;

considerato inoltre che, in un'intervista rilasciata su La7, il sottosegretario per la salute Andrea Costa ha dichiarato che si può "valutare l'ipotesi no green pass ai ristoranti dentro gli alberghi quando i ristoranti fanno un servizio esclusivo alla clientela", prevedendo l'adozione di un provvedimento in tal senso nei prossimi giorni,

si chiede di sapere se il Ministro in indirizzo intenda illustrare quali siano le soluzioni che intende adottare al fine di risolvere l'impatto negativo che il regime differenziale dell'utilizzo dei *green pass* all'interno delle strutture ricettive, di cui al decreto-legge n. 105 del 2021, sta già avendo sulle prenotazioni, ovvero se possa fornire elementi circa le valutazioni che il suo Dicastero stia compiendo relativamente alla possibilità di rimuovere l'utilizzo dei *green pass* per l'accesso ai ristoranti riservati alla clientela delle strutture ricettive, secondo quanto già anticipato dal Sottosegretario di Stato.

(3-02768)

FARAONE - *Al Ministro della salute*. - Premesso che:

il vaccino italiano di "ReiThera", sostenuto anche da finanziamenti pubblici della Regione Lazio, e da Ministero dell'università e della ricerca e CNR, ha superato con successo le fasi 1 e 2 della sperimentazione, che hanno visto coinvolti rispettivamente gruppi di 90 e 900 volontari circa;

a seguito della decisione della Corte dei conti, adottata il 20 maggio 2021, è stato però bloccato l'avvio della fase 3 della sperimentazione che, essendo quella finale, avrebbe coinvolto migliaia di volontari e necessitava pertanto di una produzione industriale del farmaco, la quale era, per l'appunto, l'oggetto dell'accordo bocciato dalla sentenza in questione e stipulato tra l'azienda di Castel Romano, il Ministero dello sviluppo economico e Invitalia;

il vaccino, pertanto, a seguito di tale impedimento normativo, non può essere sottoposto alle valutazioni di EMA e AIFA ai fini dell'approvazione;

considerato anche il più esteso sistema di impiego della certificazione verde COVID-19 deciso con il decreto-legge n. 105 del 2021, si pone con urgenza il problema di definire la posizione dei quasi mille volontari coinvolti nelle fasi 1 e 2 della sperimentazione all'interno del sistema *green pass*, poiché, non avendo questi la possibilità di ricevere un'ulteriore dose di vaccino, somministrata con uno tra i farmaci approvati, si trovano impossibilitati ad

ottenere la certificazione secondo le modalità attualmente previste dalla legge;

considerato che:

come sottolineato, l'impossibilità di procedere all'approvazione del farmaco è di natura strettamente legale, mentre i risultati delle fasi sperimentali concluse hanno dimostrato che il 99 per cento dei soggetti coinvolti, dopo la seconda dose, ha sviluppato gli anticorpi;

essendo stata riscontrata tale forte risposta immunitaria, si rende opportuno riconoscere per i volontari ReiThera un regime dedicato di assegnazione del *green pass*, il quale verrebbe appunto rilasciato coerentemente con le ragioni della sua normale erogazione, ovvero senza che ciò comporti alcun rischio per la salute di coloro cui il certificato viene attualmente riconosciuto,

si chiede di sapere se il Ministro in indirizzo non intenda procedere, nel più breve tempo possibile, a definire la posizione dei quasi mille volontari del vaccino ReiThera all'interno del sistema delle certificazioni verdi COVID-19, considerando, a tal fine, l'opportunità di prevedere una dedicata modalità di rilascio per questi soggetti, i quali, avendo sviluppato un'adeguata reazione immunitaria, possono accedere ai luoghi sottoposti all'esibizione del *green pass*, senza che ciò comporti dei rischi per la salute collettiva.

(3-02773)

DE PETRIS - *Al Ministro della transizione ecologica*. - Premesso che, a giudizio dell'interrogante:

il Consiglio dei ministri ha approvato il 29 luglio 2021 un decreto del Presidente del Consiglio dei ministri di riorganizzazione del Ministero della transizione ecologica;

il decreto accorpa gran parte delle competenze del precedente Ministero dell'ambiente e della tutela del territorio e del mare in un Dipartimento amministrazione generale pianificazione e patrimonio naturale (DiAG), creando altresì il Dipartimento sviluppo sostenibile (DiSS) e il Dipartimento energia (DiE). Appare del tutto incomprensibile l'assenza di un esplicito richiamo alle politiche climatiche, che dovrebbero rappresentare l'asse portante di ogni strategia;

la promozione di strategie di intervento idonee a governare gli effetti dei cambiamenti climatici sul piano della mitigazione e dell'adattamento diventano competenza di tutti i dipartimenti e quindi di nessuno. Si segnala in tal senso come nel nostro Paese manchi ancora un piano di adattamento ai cambiamenti climatici volto a mitigare gli effetti dei violenti fenomeni che, negli ultimi anni, colpiscono l'Italia senza sosta, lasciando intravedere ai cittadini quale sia il futuro a cui il nostro Paese sta andando incontro. Un Piano che sarebbe necessario al fine di individuare luoghi prioritari e strumenti efficaci ma che risulta assente dalle aree di competenza e di interesse del Ministero;

anche per quanto concerne il settore energetico sembrano riproporsi le dinamiche del passato, che occorrerebbe invece correggere con urgenza: le fonti rinnovabili appaiono richiamate solo frettolosamente nell'intera riorganizzazione, la quale avrebbe dovuto riflettere quel processo di transizione ecologica all'origine della trasformazione del Ministero stesso;

il provvedimento è stato definito dal Ministro in indirizzo come una "rigenerazione che consentirà di superare quegli ostacoli di origine burocratica, tecnologica e strutturale e rendere la pubblica amministrazione efficacemente al servizio dei cittadini e dell'ambiente";

in ragione di tali affermazioni mal si comprende l'inserimento, all'articolo 5, del tema dell'energia nucleare ("Il Dipartimento esercita, nelle materie di spettanza del Ministero, le competenze in materia di: mercati energetici; efficienza energetica e energie rinnovabili; impieghi pacifici dell'energia nucleare"): tema, *in primis*, la cui inclusione tra le politiche *green* che è ancora oggetto di discussione in sede europea ma, soprattutto, che va in forte contrasto con l'espressione della volontà dei cittadini italiani, che negli ultimi 40 anni, per ben due volte (con i *referendum* del 1983 e del 2011), hanno rigettato le politiche nucleari proposte dai Governi;

non è possibile pensare di aggirare in modo così sfacciato la sovranità popolare attraverso il *greenwashing* di una produzione energetica che di pulito e rinnovabile non ha nulla;

altrettanto grave la disponibilità del Ministero a facilitare i progetti di cattura e stoccaggio dell'anidride carbonica, una pratica molto discutibile che non può in alcun modo essere considerata prioritaria nel processo di transizione ecologica ed energetica;

l'inserimento di tale pratica era stata valutato nel corso della discussione sul PNRR, senza risultare convincente: il rapporto tra rischi e benefici di questo meccanismo non è ancora chiaro e risulta del tutto evidente come l'interesse di molte aziende verso tali progetti sia connesso ai possibili profitti e alla possibilità di continuare ad utilizzare fonti inquinanti nascondendo le emissioni, letteralmente, "sotto il tappeto", all'interno di serbatoi: si ricorda come l'ENI abbia in programma la realizzazione di un impianto di stoccaggio del carbonio (CCS) a Ravenna;

proprio il responsabile public affairs dell'ENI, Lapo Pistelli, ha affermato pochi giorni fa che il CCS e l'idrogeno (da metano) "sono segmenti decisivi a loro modo, ma tutti insieme, non uno contro l'altro, per poter raggiungere gli obiettivi su cui il Paese si è impegnato";

peccato che nessuna di queste due strategie sia stata approvata dal nostro Parlamento né incontri il favore della Commissione europea, che in sede di analisi del documento relativo al *recovery plan* italiano ha chiarito come "Gli investimenti nell'idrogeno saranno limitati a quello verde e non conterranno idrogeno blu né coinvolgeranno il gas naturale", allontanando la possibilità di utilizzo della cattura e stoccaggio di anidride carbonica per produrre idrogeno blu;

tale riorganizzazione, dunque, proposta da un'azienda privata (la Ernst & Young), non corrisponde affatto ai compiti delineati per il Governo e per il neonato Ministero della transizione ecologica: al contrario, ne affossa del tutto il presidio ambientale e ne mina l'integrazione con le direttrici di politica industriale ed energetica, alla base della creazione del nuovo Ministero,

si chiede di sapere:

se il Ministro in indirizzo non intenda sottoporre ad attenta valutazione e ripensamento il progetto per come risulta essere stato disegnato, apportando le correzioni indispensabili per far sì che il Ministero corrisponda a quanto delineato nel programma di Governo, dando alle politiche climatiche la priorità che rivestono nell'agenda internazionale;

se non ritenga indispensabile promuovere, come avvenuto in molti altri Paesi, uno strumento indispensabile di indirizzo e *governance* come una legge quadro sul clima;

se non intenda chiarire di quale natura siano le competenze del Dicastero in materia di "impeghi pacifici dell'energia nucleare", posto che la politica energetica nel nostro Paese non possa appoggiarsi a tale metodo dopo la netta contrarietà dei cittadini espressa nei *referendum* del 1983 e del 2011 e se non intenda chiarire la posizione del Governo circa la pratica di cattura e stoccaggio dell'anidride carbonica, molto controversa e dunque inaffidabile ai fini della pianificazione di una completa transizione ecologica della nostra economia.

(3-02774)

BINETTI - *Al Ministro dell'università e della ricerca*. - Premesso che:

al fine di poter garantire un ottimale insegnamento professionalizzante, non è più rinviabile il problema della insufficiente e precaria presenza di docenti appartenenti allo specifico profilo professionale, chiamati in ruolo da parte delle università;

sul totale di 487 docenti attualmente di ruolo nei settori scientifico-disciplinari (SSD) MED/45-50, solo 62 appartengono ai settori specifici dei profili delle 22 professioni sanitarie, pari ad appena il 13 per cento. La restante parte, circa l'87 per cento, sono in prevalenza medici e odontoiatri, alcuni biologi, farmacologi e psicologi. Lo scorso anno i docenti erano 457, trenta in meno di questo anno, a fronte dei 9.138 dell'intera area 6 di Medicina;

il settore MED/45 (Scienze infermieristiche generali) ha in ruolo 43 docenti, di cui 40, ovvero il 93 per cento, appartenenti alla professione infermieristica, i quali risultano ancora sotto-organico, se si considera l'esistenza di 42 corsi di laurea distribuiti su 217 sedi. Invero mancano professori di ruolo per il corso universitario di Infermieristica nella metà delle Università italiane, tra cui: Bologna, Parma, Ferrara, Pisa, Siena, Perugia, Ancona, Chieti, Napoli Federico II, Napoli Vanvitelli, Salerno, Campobasso, Foggia, Catanzaro, Catania, Messina, Palermo, Sassari e Cagliari;

sicuramente peggiore è la situazione nei restanti SSD: nessun insegnate di ruolo fra i 183 di MED/46 (Tecniche di laboratorio) e fra i 92 del MED/49 (Dietistica); 4 su 6 quelli di ruolo in ostetricia, 14 su 34 nel settore della riabilitazione, nonché 4 su 122 per il corso universitario MED/50 (Scienze Tecniche mediche applicate), di cui 2 igienisti dentali, 1 logopedista e 1 ortottista;

il numero dei docenti impegnati nei SSD presi in considerazione è sempre del tutto inferiore alle effettive necessità espresse dal carico della docenza dei relativi corsi di laurea;

occorre, poi, evidenziare come rispetto alle 22 professioni a cui appartengono oltre 687.000 operatori, i ruoli esistono solo per 11 delle 22 professioni di area sanitaria, quindi per la metà, ovvero: 40 ruoli per infermieri su 456.000 iscritti all'Ordine, 9 per fisioterapisti su 66.000 iscritti, 4 per ostetriche su 21.000, 2 per igienisti dentali su 8.000 e 2 per terapisti delle neuro- e psicomotricità dell'età evolutiva su 5.000. Inoltre, un ruolo ciascuno per i circa 20.000 educatori, per i 12.000 logopedisti, per i 3.000 ortottisti, per i 3.000 terapisti della riabilitazione psichiatrica e per i 2.000 tecnici di neurofisiopatologia;

mancano totalmente i ruoli per altre 12 professioni ovvero: per gli 11.000 tecnici della Prevenzione, per gli oltre 5.000 dietisti, per i circa 5.000 assistenti sanitari, per i 4.000 audioprotesisti, per i 2.250 terapisti occupazionali, per i 2.200 podologi e 2.200 tecnici ortopedici, per i 1.500 tecnici di Fisiopatologia cardiocircolatoria ed infine per i mille tecnici audiometristi. Inoltre risultano mancanti i ruoli di insegnamento per alcune tipologie di professione ad alta numerosità come per i 28.000 tecnici di Radiologia e per i 27.000 tecnici di Laboratorio;

le università con il maggior numero di ruoli non affidati a docenti appartenenti ad una delle professioni sanitarie sono la "Sapienza" di Roma con 87 ruoli, di cui solo 4 per le professioni, e la "Federico II" di Napoli con 44 ruoli e nessuno per le professioni sanitarie;

non c'è dubbio che la mancanza dei docenti provenienti dalle rispettive professioni sanitarie mostri una debolezza della ricerca scientifica in questi stessi settori, situazione questa che da una parte non consente ai docenti di accedere alle rispettive abilitazioni scientifiche nazionali e dall'altra rende intrinsecamente più deboli questi corsi di laurea in cui il livello del sapere che li caratterizza non raggiunge quello di un'adeguata elaborazione scientifica;

alla luce di quanto esposto vi è anche il dubbio che in questi trent' anni dalla istituzione di detti corsi di laurea, i docenti-professionisti non abbiano potuto contare su una formazione scientifica *ad hoc*, ovvero una sorta di accompagnamento al lavoro scientifico con possibilità di dedicare tempo reale alla attività di ricerca,

si chiede di sapere:

come intenda intervenire il Ministro in indirizzo per facilitare l'attività di ricerca dei docenti che insegnano nei SSD dedicati "ai saperi specifici" nei

rispettivi corsi di laurea, anche attraverso un aumento significativo delle borse di dottorato e delle borse *post* dottorato, al fine di favorire la formazione scientifica e la relativa produzione scientifica;

come intenda procedere nell'ambito dei concorsi pubblici per i diversi corsi di laurea, promuovendo le competenze specifiche e considerando la capacità professionale e la competenza scientifica come due fattori entrambi afferenti allo spirito accademico.

(3-02776)

RIZZOTTI - *Al Ministro della salute*. - Premesso che:

le fratture da fragilità ossea rappresentano un'emergenza sanitaria che ad oggi non riceve, sia in Italia che in Europa, adeguate risposte di sanità pubblica che l'entità di questo fenomeno richiede. Questa condizione causa disabilità complesse, con un enorme impatto sulla qualità della vita e genera anche gravi limitazioni funzionali, aumentando notevolmente il rischio di mortalità;

solo in Italia, le fratture da fragilità colpiscono 3,2 milioni di donne e 0,8 milioni di uomini *over* 50, con un previsto aumento, nei prossimi 10 anni, del 22,4 per cento. I costi sanitari associati ammontano a 9,4 miliardi di euro, con un aumento stimato del 26,2 per cento nei prossimi 10 anni (2030: 11,9 miliardi di euro). Questi dati estremamente preoccupanti emergono dal rapporto annuale prodotto dalla International osteoporosis foundation, per l'Italia e insieme ai dati prodotti per la Germania, Regno Unito, Francia, Spagna e Svezia, offrono una misura tangibile di un'emergenza -sia gestionale che terapeutica- per la quale è urgente adottare una risposta sanitaria adeguata;

l'aumento della popolazione anziana, previsto nel prossimo futuro, non potrà che aggravare ulteriormente lo scenario attuale, rendendo quanto mai indispensabili azioni concrete per la prevenzione e la riduzione dell'impatto sociale ed economico delle fratture da fragilità ossea;

le misure adottate congiuntamente dal Ministro della salute e dal Ministro dell'interno allo scopo di contrastare e contenere il diffondersi dell'infezione da COVID-19 su tutto il territorio nazionale hanno limitato molto l'attività motoria e ricreativa all'aperto, vietando l'attività fisica e riabilitativa;

l'essere, altresì, costretti a trascorrere molto tempo a casa ha indotto una parte degli italiani ad un'eccessiva sedentarietà, soprattutto gli anziani con malattie croniche, come diabete o malattie polmonari, cardiache o renali, i quali, essendo a maggior rischio di complicanze da COVID-19, dopo mesi di inattività, hanno il più elevato rischio di fratture;

per alzare il livello di attenzione sul tema della fragilità ossea, 7 società medico-scientifiche e 18 associazioni di pazienti hanno dato vita a "Frame", un'alleanza che ha prodotto un manifesto sociale, con il quale viene sollecitata l'adozione di scelte di politica sanitaria e adeguate iniziative che

consentano, attraverso nuovi modelli gestionali, di prevenire e contrastare efficacemente le fratture da fragilità ossea;

il 9 dicembre 2019 l'Agenzia europea per i medicinali (EMA) ha autorizzato la commercializzazione in Europa del farmaco Romosozumab e nel 2020 si è dato avvio alla procedura per la sua approvazione da parte dell'Agenzia italiana del farmaco;

si è venuti a conoscenza che la procedura di approvazione da parte dell'AIFA, inerente all'unico nuovo farmaco disponibile per il trattamento dell'osteoporosi, si sia conclusa senza aver raggiunto alcun accordo tra le parti, comportando sia la non rimborsabilità dello stesso da parte del sistema sanitario nazionale sia una discriminazione in termini di accesso alle cure da parte di coloro i quali convivono con questa patologia. Infatti di tale trattamento farmacologico potrebbero beneficiare solo quei cittadini ricchi in grado di comprarlo a proprie spese, mentre l'acquisto sarebbe negato a tutti coloro i quali non siano in grado di sostenere gli elevati costi che tali soluzioni terapeutiche inevitabilmente comportano;

l'impossibilità di accesso a soluzioni terapeutiche innovative in grado di migliorare la vita dei cittadini più fragili alimenterebbe un divario in termini di fruibilità dei farmaci tra l'Italia e gli altri Paesi dell'Unione europea;

l'ambito dell'osteoporosi è caratterizzato da uno scarso investimento in termini di ricerca e sviluppo e si delinea quindi un mercato che è destinato a non offrire nuove opzioni terapeutiche nei prossimi 10 anni. In tale contesto, le decisioni politiche svolgono un ruolo cruciale nel concretizzare il finanziamento per soluzioni terapeutiche innovative attraverso interventi economicamente vantaggiosi per la prevenzione delle fratture da fragilità a beneficio dei cittadini,

si chiede di sapere se il Ministro in indirizzo sia a conoscenza della questione e se ritenga di intervenire urgentemente per scongiurare ogni rischio di discriminazione nell'accesso alle cure e per tutelare il diritto alla salute di tutti i cittadini, garantendo la rimborsabilità, da parte del servizio sanitario nazionale, di soluzioni terapeutiche innovative in grado di migliorare la vita, soprattutto delle persone più fragili.

(3-02782)

Interrogazioni con richiesta di risposta scritta

RIPAMONTI, FREGOLENT, CANTÙ, LUNESU, DORIA, MARIN - *Al Ministro della salute*. - Premesso che:

sul sito dell'Istituto superiore di sanità è indicato che "la vaccinazione anti COVID-19, se si effettua il ciclo vaccinale completo, protegge all'88 per cento dall'infezione, al 94 per cento dal ricovero in ospedale, al 97 per cento

dal ricovero in terapia intensiva e al 96 per cento da un esito fatale della malattia";

più che percorrere la linea dell'introduzione di obblighi surrettizi per i cittadini, a parere degli interroganti sarebbe opportuno, attraverso una dettagliata campagna informativa, far conoscere i benefici derivanti dell'essere immunizzati e chiarire che il vaccino è una protezione utile;

una corretta informazione e la trasparenza dei dati possono aiutare i cittadini indecisi a scegliere di vaccinarsi,

si chiede di sapere se il Ministro in indirizzo non ritenga doveroso e urgente fornire, per il tramite di una circolare, delle indicazioni precise, affinché, nei dati giornalieri resi pubblici dai *media*, il numero dei positivi, degli ospedalizzati, dei ricoverati in terapia intensiva e dei deceduti sia suddiviso, per ogni singola voce, tra vaccinati con due dosi, vaccinati con una dose e non vaccinati.

(4-05886)

DE PETRIS - *Ai Ministri dell'economia e delle finanze e dello sviluppo economico*. - Premesso che:

sul quotidiano "Domani", nella versione *on line* del 28 luglio 2021 e su quella cartacea del giorno dopo, è apparso un articolo a firma del giornalista Alfredo Faieta intitolato "Vietato parlare di Eni: 'Ora dateci 100mila euro entro dieci giorni'", subito ripreso da numerose testate giornalistiche;

da quanto si evince, sembrerebbe che, in risposta ad un articolo dedicato dal giornale al procuratore generale di Milano Francesca Nanni, ENI avrebbe prima deciso di chiarire la propria posizione in una lettera inviata al direttore Stefano Feltri nella quale dissentiva riguardo ad un breve passaggio dell'articolo che toccava la società, e parallelamente avrebbe inviato al quotidiano una formale lettera di diffida tramite il proprio studio legale;

nella comunicazione, il legale si lamenterebbe della campagna diffamatoria asseritamente portata avanti da lungo tempo da "Domani" contro ENI, per poi concludere avanzando la richiesta del pagamento a titolo di previsionale del risarcimento del danno patito, quantificandola in 100.000 euro, aggiungendo peraltro che, in difetto del pagamento entro il termine perentorio di 10 giorni dal ricevimento della missiva, lo studio legale avrebbe adito le vie legali e dato corso quindi al mandato già conferito;

quella avanzata per conto di ENI dal legale incaricato sarebbe stata quindi una sorta di richiesta di danni "preventiva", che non escluderebbe ulteriori richieste risarcitorie collegate ad una successiva azione legale;

considerato che:

ENI è una società partecipata dallo Stato e sottoposta al controllo del Ministero dell'economia e delle finanze e del Ministero dello sviluppo economico;

se confermato, quanto accaduto parrebbe essere un pericoloso tentativo di condizionare e limitare la libertà di stampa e in generale il diritto ad una libera informazione,

si chiede di sapere:

se i Ministri in indirizzo, ciascuno per ciò che è di propria competenza, siano a conoscenza dei fatti esposti;

quali iniziative intendano adottare affinché ENI, quale società partecipata dallo Stato, aderisca e rispetti il principio della libertà di informazione e adotti protocolli di comportamento che siano pienamente conformi al rispetto della libertà di stampa.

(4-05887)

NUGNES - *Al Ministro delle infrastrutture e della mobilità sostenibili*. - Premesso che:

l'autostrada Pedemontana lombarda, concepita ormai decenni fa come sistema viabilistico con uno sviluppo complessivo di circa 157 chilometri, di cui 67 di autostrada, 20 di tangenziali e 70 di viabilità locale, con l'intento di collegare Bergamo con Como e Varese evitando la percorrenza delle arterie autostradali che convergono su Milano e con un costo dell'intervento che ammonterebbe a 4.118 milioni di euro, di cui 1.200 milioni di soldi pubblici e 200 milioni di prestito ponte già spesi, è un'opera progettata e dimensionata prima della crisi economica mondiale sulla base di un modello socio-economico e di sviluppo oggi radicalmente mutato;

allo stato attuale sarebbero state realizzate soltanto due tratte, la A e la B1, di collegamento Cassano Magnago (Varese), a Lentate del Seveso (Monza e Brianza), cui si aggiungono le tangenziali di Como e Varese, parte integrante del sistema viabilistico, mentre risulterebbero ancora non realizzate le tratte B2, C e D, che dovrebbero portare rispettivamente da Meda a Bovisio Masciago, poi a Vimercate e infine a Dalmine;

nel corso dell'ultima audizione dei *manager* della società Autostrada pedemontana lombarda SpA (APL) in Consiglio regionale lombardo, sarebbero emersi forti ritardi nel far partire i lavori per le tratte mancanti B2 e C, sebbene ad aprile 2021 sarebbe stato assegnato all'associazione temporanea d'imprese tra Webuild (ex Salini Impregilo), Pizzarotti e Astaldi, il bando di gara per il progetto esecutivo e la realizzazione delle tratte B2 e C, mentre per la tratta D si parlerebbe di stralcio dall'aggiornamento della progettazione definitiva, stante la difficoltà di reperire capitale privato per la sostenibilità del piano economico-finanziario, visto che la porzione di fondi pubblici definiti nel *project financing* risulterebbe già interamente spesa per realizzare le tratte A e B1 e le tangenziali di Como e Varese ora in esercizio;

nel 2017 la Regione avrebbe approvato uno stanziamento di bilancio per un fondo di garanzia ventennale da 450 milioni di euro, a partire dal 2025,

per coprire i debiti della Pedemontana con le banche dovute ai mancati introiti, al quale la stessa Regione avrebbe, a dicembre 2020, garantito l'impegno per l'incremento di ulteriori 300 milioni di euro;

ad inizio 2021 la Regione avrebbe acquisito, al costo 62 milioni di euro, l'8,03 per cento del capitale sociale di APL da Banca Intesa e l'1,54 per cento da Ubi Banca, per cui, con il controllo pari al 96 per cento da parte di Ferrovie Nord Milano (al 57,7 per cento di Regione Lombardia) e della società Milano Serravalle (MiSe), APL si caratterizzerebbe sempre più come società quasi interamente a capitale pubblico, sul quale si scarica il rischio d'impresa, mutando radicalmente il meccanismo di finanziamento misto pubblico-privato del *project financing*, sul cui presupposto doveva essere realizzata l'infrastruttura; le difficoltà nel reperire risorse economiche risiederebbero nella scarsa convenienza per i privati a concorrere con loro capitali al completamento dell'infrastruttura che rischia di non garantire un'adeguata remuneratività, stanti i ridotti volumi di traffico, rispetto alle previsioni originarie, e gli alti costi di costruzione;

per trovare ulteriori finanziatori privati APL, dopo precedenti tentativi tutti senza esito, avrebbe lanciato l'ennesima "manifestazione d'interesse", la cui fase conclusiva è stata più volte oggetto di proroga (l'attuale termine risulta spostato al 6 agosto 2021), con conseguente rinnovata dichiarazione di pubblica utilità e differimento per ulteriori 7 anni del vincolo di esproprio sulle aree interessate dal tracciato, con danno ingiusto a carico di decine di migliaia di proprietari del territorio, che da oltre 12 anni sono ostaggio di una procedura mai completata;

nel collegato alla finanziaria regionale il Consiglio regionale lombardo ha approvato la trasformazione del fondo di garanzia ventennale aperto nel 2017, in un prestito da 900 milioni di euro a APL, che si vanno ad aggiungere ai 1.200 milioni già versati dallo Stato e a mezzo miliardo di euro di defiscalizzazione, portando di fatto l'onere a carico dello Stato al 70 per cento del costo dell'opera;

considerato che:

i vincoli dimensionali di un tracciato progettato molti anni fa comportano investimenti non sostenibili né tantomeno remunerativi, stante il traffico reale atteso, come dimostrato dalla reticenza delle banche a concedere il proprio supporto pure a fronte di contributi eccezionali offerti dal Governo (1,2 miliardi di euro di finanziamento in capitale e la defiscalizzazione) e dalla Regione pronta a concedere l'ennesimo regalo alla società APL;

il completamento delle tratte mancanti, oltre all'ingente aggravio di costi a carico della finanza pubblica, produrrebbe danni consistenti ed irreparabili ad un territorio già fortemente antropizzato e urbanizzato, senza tacere dei gravi rischi ambientali derivanti dal problema della diossina TCDD, prodotta dal disastro dell'ICMESA e presente sulla tratta B2 (da Meda a Bovisio Masciago), a fronte di un progetto operativo di bonifica "al risparmio", largamente insufficiente e comunque rischioso a causa della movimentazione di terreno contaminato;

per le tratte A e B1 già in esercizio, oltre al bilancio economico insostenibile, con percorrenze ben lontane da quelle inizialmente previste, si è dovuto registrare un bilancio ambientale disastroso con la devastazione del bosco della Moronera a Lomazzo, il dimezzamento di quello della Battù a Lazzate e con la distruzione di estese porzioni di territorio agricolo di qualità, cui va aggiunto il mancato completamento di tutte le compensazioni ambientali previste, alcune delle quali sono state ridotte o snaturate rispetto al progetto originale;

come più volte dichiarato nel corso del dibattito parlamentare dagli esponenti del Governo, il piano nazionale di ripresa e resilienza rappresenta un'occasione irripetibile per operare nel nostro Paese quella "rivoluzione verde e transizione ecologica", che dovrebbe contemplare quale scelta strategica la realizzazione di adeguate infrastrutture al servizio di un nuovo modello di mobilità, moderna e sostenibile, in grado di contribuire in modo determinante al raggiungimento degli obiettivi di riduzione delle emissioni di anidride carbonica fissati dal *green deal* europeo,

si chiede di sapere:

se il Ministro in indirizzo sia a conoscenza dei fatti e delle circostanze esposti;

se non ritenga di dover disporre una puntuale verifica in merito al rispetto degli obblighi da parte della concessionaria Autostrada pedemontana lombarda SpA e all'ammontare delle risorse pubbliche fin qui spese per la costruzione parziale dell'infrastruttura;

se il Governo intenda valutare l'opportunità di stralciare l'autostrada Pedemontana lombarda dalle opere strategiche definite di interesse nazionale e di dirottare le risorse risparmiate per procedere esclusivamente al potenziamento della Milano-Meda, sempre a percorrenza gratuita, per rispondere alle evidenti criticità di saturazione veicolare, al potenziamento o la ricreazione di assi ferroviari come quello tra Bergamo, Lecco, Como e Varese sui quali spostare il trasporto sia di merci che di persone, nonché il potenziamento del servizio di trasporto pubblico e la connessione tra l'area metropolitana e vimercatese con il prolungamento della M2 da Cologno a Vimercate e la creazione di collegamenti con le stazioni ferroviarie di Arcore e Usmate-Carnate.

(4-05888)

ROMANO, MATRISCIANO, CATALFO, GUIDOLIN, ROMAGNOLI, CASTELLONE, DELL'OLIO, LUPO, CROATTI, DONNO, TAVERNA, GIROTTO, L'ABBATE, MANTOVANI, NOCERINO, MARINELLO, RICCIARDI, PRESUTTO, CORBETTA, AIROLA, VACCARO, AUDDINO, BOTTICI, LANZI, QUARTO, GAUDIANO, COLTORTI, CAMPAGNA, VANIN, NATURALE, PESCO, GALLICCHIO, LEONE, CASTALDI, PISANI Giuseppe, DI PIAZZA, FERRARA, MONTEVECCHI, PIRRO, PUGLIA, MAIORINO, CIOFFI, PIARULLI, D'ANGELO,

EVANGELISTA, TURCO, PAVANELLI, FENU, SANTILLO, PELLEGRINI Marco, MAUTONE, TRENTACOSTE, FEDE - *Al Ministro della giustizia*. - Premesso che:

le previsioni normative sui controlli afferenti all'erogazione del reddito di cittadinanza coinvolgono più istituzioni, tra cui il Ministero della giustizia;

più nello specifico, ai sensi dell'articolo 5, comma 3, del decreto-legge n. 4 del 2019, ai fini del riconoscimento della misura, l'INPS è tenuto a verificare il possesso dei requisiti necessari sulla scorta delle informazioni disponibili nei propri archivi e in quelli di altre pubbliche amministrazioni titolari dei dati richiesti;

ai sensi del decreto del Presidente della Repubblica n. 445 del 2000 l'Istituto effettua i dovuti accertamenti sulle dichiarazioni prodotte dai richiedenti il reddito di cittadinanza, sia in fase istruttoria, al momento della presentazione, che in esito all'accoglimento;

a tal fine, sono previsti controlli sincroni automatizzati sui requisiti di residenza, possesso di beni durevoli, stato lavorativo e situazione reddituale del nucleo familiare e tali controlli consentono di anticipare la verifica delle autodichiarazioni, con parere conforme del Garante per la protezione dei dati personali, sulla base delle previsioni di legge e nel rispetto delle regole di cui al disciplinare sui controlli, adottato dall'INPS con determinazione n. 95/2020;

considerato che:

con riferimento specifico alle dichiarazioni rese dai richiedenti il reddito di cittadinanza inerenti all'assenza di eventuali misure cautelari personali, anche adottate a seguito di convalida dell'arresto o del fermo, e di condanne definitive intervenute nei 10 giorni precedenti per i reati richiamati dall'articolo 7, comma 3, del decreto-legge n. 4, al momento sono effettuati solo controlli *ex post* a campione presso gli uffici del casellario giudiziario, atteso che la platea dei beneficiari la misura non consente un controllo diffuso e massivo per tutti i componenti del nucleo familiare;

per arginare il fenomeno delle prestazioni erogate indebitamente a soggetti per i quali emerga solo successivamente al riconoscimento del beneficio l'assenza dei requisiti di legge, l'INPS ha in atto collaborazioni con la Guardia di finanza;

sarebbe opportuno intervenire già *ex ante* nei controlli utili ad intercettare potenziali indebiti accessi al beneficio del reddito di cittadinanza;

stipulare un'apposita convenzione con il Ministero della giustizia ai fini dell'individuazione preventiva dei soggetti non aventi titolo al beneficio permetterebbe un'azione più efficace ed efficiente, evitando, altresì, le problematiche legate al recupero di quanto indebitamente percepito,

si chiede di sapere se e quali iniziative il Ministro in indirizzo intenda adottare affinché il Ministero sottoscriva apposita convenzione con l'INPS per

lo scambio massivo delle informazioni detenute e utili all'istruttoria dovuta per legge e, in difetto, quali eventuali circostanze impediscano tale scambio.

(4-05889)

FREGOLENT - *Al Ministro della salute*. - Premesso che:

il tema del passaporto vaccinale ha popolato le agende politiche delle ultime settimane e i tavoli di lavoro aperti al riguardo sono diversi, portando all'attenzione il rischio che il *green pass* finisca per essere un elemento di discriminazione, dividendo i cittadini tra chi può iniziare a muoversi liberamente e chi no;

il *green pass* si ottiene in presenza di una di queste tre condizioni, alternative tra loro: aver avuto il COVID ed esserne guariti: in questo caso in certificato avrà validità di 6 mesi a decorrere dalla data di emissione; aver effettuato un tampone rapido o molecolare risultato negativo nelle 48 ore precedenti all'utilizzo del certificato: in questo caso la validità è limitata all'evento per cui viene esibito; aver ricevuto almeno una dose di vaccino. In questo caso il *pass* si ottiene dopo 15 giorni dalla prima dose, o immediatamente dopo la seconda, ed ha validità di 9 mesi a partire dalla seconda dose;

tra le condizioni indicate, non vi è quella in ordine all'effettuazione di un *test* sierologico che individui la presenza di anticorpi al coronavirus, che provano una copertura vaccinale protratta nel tempo, registrando valori superiori di anticorpi anche di chi ha fatto le due dosi;

a questi soggetti viene tolta la libertà di viaggiare, di partecipare ad un evento nonostante abbiano una copertura vaccinale, venendo considerati alla stregua di soggetti senza copertura vaccinale, costretti, così, ogni 2 giorni a farsi un tampone per tornare alla normalità;

invero, il sistema attuale riconosce il *green pass* solo a coloro che sono guariti e a cui è stata rilasciata una certificazione dalla struttura presso la quale è avvenuto il ricovero del paziente affetto da COVID-19, ovvero, per i pazienti non ricoverati, dai medici di medicina generale e dai pediatri di libera scelta, ed è resa disponibile nel fascicolo sanitario elettronico dell'interessato;

non vengono presi in considerazione, dunque, tutti quei soggetti che, ad esempio, sono stati positivi asintomatici e hanno scoperto di aver contratto il virus solo a seguito dell'effettuazione del *test* sierologico, e nelle more non possono effettuare il vaccino poiché controindicato a fronte dell'alta quantità di anticorpi rilevati,

si chiede di sapere se il Ministro in indirizzo non ritenga doveroso e urgente individuare misure specifiche per coloro che presentano tali condizioni, prevedendo che tra le condizioni per cui si ottiene il *green pass* sia inserita anche l'ipotesi di coloro che, seppure non in possesso di un certificato di guarigione, hanno effettuato un *test* sierologico, che dimostri la presenza di anticorpi al virus e dove la lettura dell'anamnesi completa suggerisca la non effettuazione del vaccino.

(4-05890)

BARBONI, BERNINI, AIMI, PAGANO - *Al Ministro dell'interno*. - Premesso che:

dal 17 giugno 2021 è entrata in vigore la legge n. 84, sul distacco dei Comuni di Montecopiolo e Sassofeltrio dalla Regione Marche e loro aggregazione alla Regione Emilia-Romagna, nell'ambito della provincia di Rimini, ai sensi dell'articolo 132, secondo comma, della Costituzione;

la legge n. 84 del 2021 è stata approvata dal Senato della Repubblica dopo un lungo *iter* iniziato con il *referendum* svoltosi nel 2007, a seguito del quale l'83 per cento degli abitanti di Montecopiolo e l'87 per cento degli abitanti di Sassofeltrio si sono espressi favorevolmente per il passaggio dei due Comuni dalla provincia di Pesaro-Urbino a quella di Rimini;

in base all'art. 1 i due Comuni interessati possono distaccarsi dalla Regione Marche e aggregarsi alla Regione Emilia-Romagna in considerazione della loro particolare collocazione territoriale e dei peculiari legami storici, economici e culturali con i comuni limitrofi della provincia di Rimini;

entro 30 giorni dalla data di entrata in vigore della legge, il Ministro dell'interno, con proprio decreto, nomina un commissario, a tutela del passaggio, con il compito di promuovere gli adempimenti necessari per l'attuazione dell'art. 1;

il commissario deve essere nominato dal Ministro dell'interno, sentite le Regioni Marche ed Emilia-Romagna e la Provincia di Rimini, che devono altresì provvedere agli adempimenti di rispettiva competenza, oltre a quelli necessari per l'attuazione dell'art. 1, nel rispetto del principio di leale collaborazione, attraverso accordi, intese e atti congiunti, garantendo continuità nelle prestazioni e nelle erogazioni di servizi;

come previsto dall'art. 2, comma 4, il commissario nominato deve assicurare che gli adempimenti necessari siano posti in essere entro un anno dall'entrata in vigore della legge;

nonostante siano decorsi i 30 giorni dall'entrata in vigore della legge n. 84 del 2021 non risulta sia stata attivata la procedura per la nomina del commissario,

si chiede di sapere se il Ministro in indirizzo abbia predisposto gli atti necessari per la nomina del commissario alla tutela del passaggio, atto necessario sancito dalla legge, per l'aggregazione dei Comuni di Montecopiolo e Sassofeltrio alla Provincia di Rimini.

(4-05891)

FAZZOLARI - *Al Ministro della salute*. - Premesso che:

come è noto, l'articolo 3 del decreto-legge 23 luglio 2021, n. 105, recante "Misure urgenti per fronteggiare l'emergenza epidemiologica da Covid-

19 e per l'esercizio in sicurezza di attività sociali ed economiche", ha disposto che a far data dal 6 agosto 2021 una lunga serie di attività e servizi sarà consentita in zona bianca esclusivamente alle persone, di età superiore agli anni 12, munite di una delle certificazioni verdi COVID-19 previste dalla vigente normativa;

a decorrere da tale data il *green pass*, già necessario per muoversi in tutta Europa, sarà richiesto in Italia a tutti gli *over* 12 in zona bianca per l'accesso ad eventi sportivi, fiere, piscine, palestre, congressi, musei, parchi tematici e di divertimento, limitatamente alle attività al chiuso, e sarà richiesto altresì per sedersi ai tavoli di ristoranti, bar, cinema, centri termali e sale bingo al chiuso ed addirittura per partecipare a concorsi pubblici;

tali disposizioni si applicano anche nelle zone gialla, arancione e rossa, laddove i servizi e le attività siano consentiti ed alle condizioni previste per le singole zone;

il *green pass* è però attualmente rilasciato, come è noto, esclusivamente a seguito all'avvenuta vaccinazione con vaccini approvati dall'EMA, e la circostanza della sua fattuale obbligatorietà a decorrere dal 6 di agosto determina, comprensibilmente, forte preoccupazione per gli abitanti della Repubblica di San Marino, dove è stata implementata una massiva campagna vaccinale che solo qualche giorno fa ha determinato il raggiungimento della cosiddetta immunità di gregge con il 70 per cento della popolazione vaccinata, di cui il 90 per cento con il vaccino russo Sputnik;

il problema riguarda circa 15.000 italiani residenti sul Titano, i quali, dopo i pesanti contraccolpi subiti dapprima a causa della questione legata al "*caos* targhe" (conseguenza diretta del "decreto sicurezza"), e dopo l'aggravarsi della situazione epidemiologica locale a causa del ritardo nella consegna delle dosi dei vaccini promesse dall'Italia, ora sono alle prese con gli effetti negativi del nuovo decreto COVID che limita i loro spostamenti,

si chiede di sapere quali soluzioni il Ministro in indirizzo ritenga di individuare al fine di evitare ingiuste penalizzazioni e ulteriori ripercussioni legate alla gestione della crisi pandemica ai danni dei cittadini di San Marino, vaccinati in larghissima maggioranza con il vaccino Sputnik, in relazione all'impossibilità di ottenere il rilascio del *green pass*, di fatto obbligatorio per una larga serie di attività sociali e servizi a decorrere dal 6 agosto 2021.

(4-05892)

ROJC - *Ai Ministri dell'istruzione e per gli affari regionali e le autonomie*. - Premesso che:

l'ufficio per l'istruzione in lingua slovena presso l'ufficio scolastico regionale del Friuli-Venezia Giulia ha inviato una nota ai dirigenti scolastici interessati (delle scuole con lingua d'insegnamento slovena), al fine di verificare la possibilità di recuperare ore d'organico (del cosiddetto organico di fatto) in esecuzione di precise indicazioni ricevute dalla locale direzione regionale;

tali indicazioni sarebbero state disposte unilateralmente e d'autorità, in violazione delle vigenti norme circa la competenza sulla definizione degli organici delle scuole con lingua d'insegnamento slovena, che radicano, sin dal 2009, tale competenza in capo all'ufficio per l'istruzione in lingua slovena;

la decisione di non assegnare l'organico di fatto per le (sole) scuole con lingua d'insegnamento slovena risulta non solo illegittima (con riferimento alle competenze amministrative citate) ma persino illecita, perché contraria alle vigenti norme di tutela della minoranza slovena, a loro volta supportate da trattati internazionali ed accordi bilaterali tra Italia e Slovenia. Risulta, viceversa, che non siano state date indicazioni di stampo analogo per le scuole italiane, alle quali verrà garantito l'organico di fatto (né potrebbe essere altrimenti), pena il mancato avvio dell'anno scolastico;

considerato che:

la decisione della direzione generale dell'ufficio scolastico regionale del Friuli-Venezia Giulia, in difetto di specifiche prescrizioni di legge che dispongano (*rectius*, che consentano) una simile discriminazione tra scuole italiane e scuole slovene (delle quali si chiede conto, nella denegata ipotesi che siano state emanate dal Ministero dell'istruzione) senza alcuna ragione di natura tecnica, ponendosi in aperto contrasto con le vigenti norme in materia, richiede un intervento urgente così come si avverte la netta sensazione che, in assenza di disposizioni di legge o di indicazioni ministeriali nel senso intrapreso dalla direzione generale dell'ufficio scolastico regionale, una simile decisione, gravissima nei modi e nei termini laddove confermata, assuma tratti di natura squisitamente politica, posto che la specificità del sistema di istruzione in lingua slovena è ben noto e sarebbe davvero bizzarro apprendere che non ne siano a conoscenza presso la direzione generale dell'ufficio scolastico regionale del Friuli-Venezia Giulia;

appare tanto più grave un simile comportamento in assenza di precise indicazioni in tal senso da parte del Ministero dell'istruzione,

si chiede di sapere:

se i Ministri in indirizzo non ritengano, in ragione della gravità dei fatti laddove confermati, di adottare le iniziative di competenza volte a sensibilizzare i vertici della direzione generale dell'ufficio scolastico regionale del Friuli-Venezia Giulia affinché assicurino la piena applicazione ed il rispetto delle vigenti norme non solo in materia di tutela della minoranza slovena, ma in particolare le norme emanate dallo stesso Ministero dell'istruzione sull'argomento, a partire dall'art. 21 del decreto del Presidente della Repubblica n. 81 del 2009;

quali iniziative urgenti intendano intraprendere, considerato che la questione è stata posta all'ordine del giorno nella recente riunione del tavolo permanente sulle questioni attinenti la minoranza linguistica slovena in Italia (di cui al decreto ministeriale 4 luglio 2012), tenutosi a Trieste in data 2 luglio 2021 alla presenza del Sottosegretario di Stato per l'Interno Scalfarotto, al fine

di affrontare in maniera risoluta, oltre che definitiva, il riconoscimento formale delle competenze dell'ufficio per l'istruzione in lingua slovena, istituito con la legge n. 38 del 2001.

(4-05893)

PRESUTTO, SANTILLO, GALLICCHIO, VACCARO, VANIN, CROATTI, ROMANO, TRENTACOSTE - *Al Ministro delle infrastrutture e della mobilità sostenibili*. - Premesso che:

la galleria Vittoria, snodo nevralgico di vitale importanza per la città di Napoli, è da diverso tempo chiusa al traffico a causa del suo stato di degrado, caratterizzato da numerosi distacchi di materiale murario determinatisi a causa delle numerose infiltrazioni;

la galleria, attualmente considerata pericolosa per la pubblica incolumità, riveste un ruolo fondamentale nella gestione delle emergenze del Ccomune di Napoli, in quanto parte degli itinerari previsti dai piani della protezione civile per l'evacuazione della città e dell'area metropolitana, con conseguenti notevoli ripercussioni sia per l'interno sistema stradale cittadino che sulla capacità di afflusso alle stazioni metropolitane e ferroviarie;

lo storico *tunnel* rappresenta uno strumento viario non evitabile e, da quando è chiuso, la città appare divisa in due con gli immaginabili pesanti contraccolpi per la viabilità;

andando a ritroso nel tempo ci si accorge che la struttura è stata oggetto di numerosi provvedimenti amministrativi che però non hanno condotto, ad oggi, alla risoluzione dei problemi;

con deliberazione di Giunta comunale n. 87 del 2 marzo 2018, constatato lo stato di degrado della struttura, è stato approvato un progetto di fattibilità tecnica ed economica inerente la "messa in sicurezza definitiva ed il restauro delle facciate della galleria" per un importo di 1.600.000 euro. In data successiva rispetto all'aggiudicazione dell'appalto, tuttavia, è emersa la necessità di prevedere altri interventi non considerati nella progettazione originaria a seguito di un ulteriore peggioramento dello stato manutentivo del bene monumentale;

alla luce delle nuove risultanze, la Giunta comunale ha approvato con delibera n. 575 del 29 novembre 2019 un nuovo intervento per un importo pari a circa 2.000.000 euro, concretizzatosi nella successiva approvazione del progetto esecutivo per mezzo della deliberazione n. 624 del 20 dicembre 2019;

ancora una volta, con deliberazione di Giunta comunale n. 218 del 17 febbraio 2020, si è provveduto ad approvare una variazione di bilancio provvisorio in corso di gestione 2020-2022 per utilizzare ai fini del restauro della galleria una quota dell'avanzo di amministrazione pari a 541.000 euro circa, in precedenza destinati ad altri interventi;

nella notte del 23 settembre 2020 in conseguenza del distacco di uno dei pannelli di rivestimento della galleria l'amministrazione comunale ha disposto la chiusura parziale della struttura;

a seguito dei necessari sopralluoghi, infatti, il servizio di protezione civile del Comune ha disposto la chiusura della carreggiata in direzione di piazza Vittoria demandando al servizio strade e grandi reti tecnologiche le successive verifiche sull'intera galleria, finalizzate ad accertare lo stato dei supporti metallici dei pannelli del rivestimento;

l'autorità giudiziaria, in data 24 settembre 2020, ha disposto il sequestro dell'infrastruttura;

a seguito dei rilievi della magistratura, il Comune ha avviato specifiche indagini per verificare lo stato di stabilità della struttura e di conservazione dei pannelli, culminate con la delibera di Giunta n. 480 del 29 dicembre 2020 per mezzo della quale è stato approvato un progetto di rifunzionalizzazione della struttura con un *budget* di 600.000 euro. Il Comune ha in seguito individuato una ditta per l'esecuzione dei lavori;

per dare inizio ai lavori, il Comune ha chiesto all'autorità giudiziaria il dissequestro della galleria. L'intenzione era quella di lavorare su una carreggiata lasciando aperta al traffico l'altra;

l'autorità giudiziaria ha però negato il dissequestro evidenziando come il progetto del Comune non fosse stato in grado di comprendere quale fosse l'origine delle infiltrazioni e come le verifiche di tenuta e sicurezza operate fossero state condotte solo "su base qualitativa e non visiva" senza di fatto eliminare il "potenziale pericolo per la comunità". Mentre l'autorità giudiziaria bocciava il progetto, tuttavia, lo stesso Comune annunciava, stranamente, l'apertura della galleria entro la primavera 2021;

il dissequestro della struttura, per un periodo limitato di 4 mesi, è stato disposto solo in data 13 aprile 2021. A seguito di ciò il Comune ha redatto un ulteriore progetto esecutivo per la messa in sicurezza e l'esecuzione dei lavori, approvato con deliberazione di Giunta n. 229 del 1° giugno 2021, denominato "manutenzione straordinaria finalizzata alla rifunzionalizzazione della galleria Vittoria";

con delibera di Giunta comunale n. 264 del 26 giugno 2021 si è deciso di affidare ad ANAS la realizzazione degli interventi di manutenzione per un investimento complessivo pari a 2.000.000 euro, cifra ben lontana dai 600.000 euro previsti mesi prima dal Comune per le medesime finalità;

ad oggi la galleria è ancora chiusa al traffico e ciò, come già specificato, determina smisurati disagi alla circolazione viaria. Secondo ANAS i tempi di ripristino saranno di circa 4 mesi, a partire dal 2 agosto 2021;

a parere degli esperti, tuttavia, ci vorrà un anno e mezzo per il recupero completo della struttura. Per rispondere alle richieste della Procura, occorrerà andare a cercare le cause delle infiltrazioni verificatesi nel tempo e, per fare ciò, non esiste altra possibilità che rimuovere il rivestimento interno che ha funzione di "controsoffitto" e serve proprio a fermare le acque di infiltrazione;

i pannelli esterni oggi visibili sono stati posizionati negli anni '60, al di sopra di una precedente copertura. La vecchia copertura ha ceduto in più punti determinando un'occlusione dei canali di raccolta delle acque che si trovano all'interno dell'attuale rivestimento. Queste occlusioni hanno inoltre corroso i ganci di acciaio che sorreggono i pannelli. Per ripulire occorrerà, quindi, rimuovere un doppio strato di pannelli, trovare la causa dell'infiltrazione e ricostruire;

alla già travagliata storia della galleria si è aggiunto di recente un altro tassello: una seconda indagine giudiziaria avviata nei confronti degli uffici tecnici del Comune di Napoli, raggiunti da una nuova richiesta di accertamenti da parte della Procura;

tale inchiesta, a differenza della precedente, mira a fare chiarezza sulla gestione degli interventi di manutenzione messi a segno negli anni precedenti al 2020 nel tentativo di verificare eventuali errori o omissioni: si intende indagare in merito a tutti i procedimenti amministrativi, progetti, lavori e appalti che dal 2014 in poi hanno scandito la storia del *tunnel*, facendo luce su eventuali omissioni di atti di ufficio nella trafila di procedimenti amministrativi adottati negli anni scorsi;

le due indagini giudiziarie condotte in parallelo appaiono come due facce della stessa medaglia e vedono come protagonista un bene essenziale per la città di Napoli,

si chiede di sapere:

se il Ministro in indirizzo sia a conoscenza dei fatti esposti;

come intenda intervenire per far luce sulle intricate vicende che hanno caratterizzato la storia della galleria Vittoria, al fine di individuare eventuali responsabilità nella gestione della sua manutenzione;

se intenda attivarsi per far sì che lo snodo viario di primaria importanza venga al più presto restituito alla città in condizioni di assoluta sicurezza.

(4-05894)

ASTORRE, FEDELI, MARGIOTTA, ROJC, STEFANO, D'ALFONSO, BOLDRINI, GIACOBBE, PITTELLA, LAUS, TARICCO, COLLINA, ROSSOMANDO, FERRAZZI, MANCA, VALENTE, PINOTTI, D'ARIENZO, CIRINNÀ - *Al Ministro delle infrastrutture e della mobilità sostenibili*. - Premesso che:

il settore crocieristico è stato tra i più colpiti dall'emergenza sanitaria da COVID-19. Il crollo verticale della domanda, nel 2020 il calo dei passeggeri ha sfiorato il 95 per cento, ha generato perdite considerevoli per l'intero comparto, e conseguentemente per l'economia italiana legata al turismo;

il Governo, consapevole della drammatica situazione del comparto crocieristico, ha varato alcuni provvedimenti finalizzati a ristorare dalle perdite subite, pur consapevole che tali ristori non avrebbero mai compensato il totale delle perdite;

con l'ultimo provvedimento, approvato dalle Camere recentemente (cosiddetto "decreto sostegni-*bis*"), il Governo ha introdotto alcune misure destinate a sostenere, per quanto possibile, il settore. Si tratta dell'incremento del fondo, da 5 a 10 milioni di euro per il ristoro delle città portuali, e la sospensione temporanea della tassa di ancoraggio per le navi da crociera, con contestuale istituzione di un Fondo, con una dotazione pari a 2,2 milioni di euro per l'anno 2021, che sarà diretto alla compensazione delle Autorità di sistema portuale per i mancati introiti della tassa suddetta;

considerato che:

il porto di Civitavecchia, primo porto crociere d'Italia, il più duramente colpito dal COVID-19, con un crollo dei passeggeri nel 2020 quasi del 100 per cento, pur con tutti gli sforzi che sta compiendo l'Autorità di sistema portuale, sotto il profilo amministrativo e contabile, per garantire una gestione e una organizzazione efficiente e, in prospettiva, in grado di riprendere a pieno le proprie attività, rischia seriamente di compromettere i servizi crocieristici e di non garantire i livelli occupazionali;

recentemente, il Comitato di gestione ha approvato l'assestamento del bilancio di previsione 2021. Una manovra da oltre 1 milione di euro, resasi possibile grazie ad interventi di razionalizzazione delle spese, tra cui le spese per il personale, e al contributo di maggiori entrate per le soste inoperose delle navi da crociera. Tuttavia, a fronte di un'operazione sull'assestamento del bilancio di previsione 2021 improntata alla prudenza, finalizzata alla messa in sicurezza dei conti per il 2021, lo scenario, in prospettiva, senza un concreto sostegno del Governo, desta molte preoccupazioni,

si chiede di sapere:

alla luce di quanto riportato in premessa, se il Ministro in indirizzo non ritenga opportuno accelerare la fruibilità di tutte quelle risorse approvate dal Parlamento e dal Governo a sostegno del settore crocieristico;

se non ritenga utile considerare l'ipotesi di una misura *ad hoc* per il solo comparto crocieristico nazionale.

(4-05895)

LAFORGIA, DE PETRIS, BUCCARELLA, ERRANI, RUOTOLO - *Ai Ministri del lavoro e delle politiche sociali e dello sviluppo economico*. - Premesso che:

da organi di stampa si apprende che Logista, la multinazionale monopolista nella distribuzione del tabacco, ha deciso di chiudere il sito di Bologna e ha avvisato tutti i lavoratori con un messaggio via "WhatsApp" inviato sabato 31 luglio verso le ore 22;

la comunicazione è arrivata senza alcun preavviso e senza alcun coinvolgimento delle rappresentanze sindacali, lanciando nell'angoscia circa 90 lavoratori e le loro famiglie;

considerato che nessun dipendente in questi due anni di pandemia si è mai fermato a riposare, perché i tabacchi, si sa, sono considerati attività essenziale. Persino di fronte allo scoppio di un focolaio pandemico la multinazionale non ha chiuso un solo giorno;

ritenuto che, a parere degli interroganti, non è accettabile quanto riportato, in quanto si tratta di un metodo di comunicazione inqualificabile, che purtroppo si sta ripetendo e che calpesta i diritti e la dignità dei lavoratori che resteranno senza occupazione,

si chiede di sapere che cosa i Ministri in indirizzo intendano fare, per garantire la salvaguardia occupazionale dei lavoratori, scongiurando la chiusura dello stabilimento, e se non vogliano promuovere, d'intesa con le organizzazioni sindacali, misure che contemplino, in qualsiasi momento, il rispetto etico delle aziende nei confronti delle lavoratrici e dei lavoratori, per evitare che episodi di questa gravità possano ripetersi.

(4-05896)

BRIZIARELLI - *Al Ministro delle politiche agricole alimentari e forestali*. - Premesso che:

ad inizio 2020 un'importante operazione antimafia nell'ambito di presunte frodi ai danni dell'Unione europea ha fatto emergere un esteso fenomeno di illegalità che interessa ormai da anni tutto il territorio italiano, noto come "mafia dei pascoli";

diverse sono le aziende del Nord del Paese che continuano ad affittare dai comuni appenninici i terreni ad uso civico per ottenere fondi europei, senza di fatto svolgere effettivamente alcuna delle attività agricole o di pastorizia previste quale requisito per l'accesso ai fondi;

con tale meccanismo illegale vengono sottratte notevoli risorse, ma anche estesi terreni agli allevatori locali, che si trovano in tal modo a soffrire di scarsa disponibilità di pascoli e di aiuti europei;

i requisiti per ottenere i finanziamenti europei si basano in particolare sui titoli e sugli ettari di terreno interessati e non sull'effettiva produttività che ne deriva, in termini di pascoli e di produzione agricola;

questa pratica, oltre a consentire alle aziende interessate di percepire indebitamente il contributo della PAC, comporta un considerevole aumento dei canoni di affitto delle zone montane favorendo i grandi gruppi e le cooperative di fuori regione, rispetto ai piccoli allevatori locali;

il fenomeno risulta essere molto esteso e riguarda, ormai da anni, gran parte del territorio italiano coinvolgendo aziende e territori tra il Nord e il Sud del Paese, nelle zone che vanno dalla Valcamonica alla Valtellina, dalla val Trompia al Piemonte, al Cadore all'Umbria, all'Abruzzo, fino alla Sicilia;

il libro di Giannandrea Mencini, "Pascoli di Carta", pubblicato recentemente, dimostra la dimensione e la portata di tale problematica, descrivendo realtà di illegalità fatte di situazioni paradossali, leggi comunitarie distorte, truffe e fiumi di denaro per attività agricole e di pastorizia pressoché inesistenti;

considerato che:

a livello di fondi europei, la politica agricola comune rappresenta il 40 per cento delle spese dell'intero *budget* comunitario, e, secondo una recente analisi condotta dall'Ufficio valutazione d'impatto del Senato della Repubblica risulta che, tra il 2014 e il 2020, l'Unione europea ha accantonato per l'Italia risorse finanziarie pari ad oltre 77 miliardi di euro, di cui 46,5 miliardi per politiche di coesione e 31 miliardi per la politica agricola comune quali contributi allo sviluppo rurale;

la pandemia di coronavirus ha impattato in maniera drammatica sul settore agricolo e sulla pastorizia, che pertanto ha necessità di un supporto concreto per consentire una giusta e pronta ripresa e ripartenza, a garanzia anche dell'approvvigionamento alimentare della UE e quindi della salute e del benessere dei cittadini,

si chiede di sapere quali misure il Ministro in indirizzo intenda mettere in atto, a tutela dei legittimi allevatori e agricoltori, per garantire un controllo sull'accesso ai fondi europei nel settore agricolo nel nostro Paese e sul loro effettivo utilizzo, soprattutto per prevenire i fenomeni illeciti che ogni anno mettono a rischio il necessario supporto finanziario alle giovani e oneste imprese italiane e consentire il rilancio delle attività e dell'economia.

(4-05897)

RAUTI, CIRIANI, BALBONI, BARBARO, CALANDRINI, DE BERTOLDI, FAZZOLARI, GARNERO SANTANCHÈ, IANNONE, LA PIETRA, MAFFONI, MALAN - *Al Ministro dell'istruzione*. - Premesso che:

gli ultimi dati ISTAT disponibili, riferiti all'anno 2019, mostrano che in Italia la percentuale di giovani che abbandonano precocemente i percorsi di istruzione e formazione è pari al 13,5 per cento, un tasso ben al di sopra di quello della media degli Stati dell'Unione europea, attestato al 10,2 per cento; dalla relazione di monitoraggio del settore dell'istruzione e della formazione 2020 della Commissione europea emerge, inoltre, che un terzo (32,5 per cento) dei giovani che in Italia abbandonano precocemente gli studi e la formazione (18-24 anni) sono nati all'estero;

inoltre, dai dati ufficiali forniti dal Ministero dell'istruzione nel rapporto sulla dispersione scolastica nell'anno scolastico 2016/2017 e nel passaggio all'anno scolastico 2017/2018, pubblicato nel 2019, l'abbandono degli studi è particolarmente frequente tra gli studenti nati all'estero in Stati come l'Egitto, il Pakistan, il Bangladesh, il Senegal e la Costa d'Avorio, tutti a maggioranza musulmana, e, sul punto, una ricerca effettuata nel 2017 dall'associazione Acmid- Donna *onlus*, il cui scopo è la tutela dei diritti delle donne

musulmane in Italia, segnalava che, in Italia, 60 bambine musulmane su 1000 sono costrette dai genitori ad abbandonare la scuola dell'obbligo tra la quinta elementare e la prima media, un dato estremamente preoccupante che tra il 2016 e il 2017 era triplicato;

considerato che:

l'abbandono scolastico da parte delle bambine di fede islamica è un problema diffuso su tutto il territorio nazionale ed è una condizione in cui versano migliaia di minori in Italia, mentre colpisce in misura decisamente inferiore i coetanei maschi; l'emergenza pandemica e la necessità di ricorrere alla didattica a distanza notoriamente hanno causato disagio alla popolazione scolastica e soprattutto alle fasce sociali più fragili, causando, nel 2020, il mancato ritorno a scuola di 200.000 studenti; anche l'anno scolastico 2020/2021 ha visto alternarsi numerosi periodi di didattica a distanza e, dunque, verosimilmente si realizzerà il medesimo *trend* di abbandono, soprattutto nelle fasce più fragili;

inoltre, si può ritenere che la didattica a distanza abbia penalizzato fortemente anche le bambine di fede islamica, e appare verosimile che il loro tasso di abbandono scolastico possa andare incontro ad un incremento; i giovani che lasciano gli studi precocemente sono destinati a diventare NEET (*not in employment, education and training*), termine con il quale si indicano gli individui con un'età compresa tra i 15 ed i 29 anni che non studiano e non lavorano;

il diritto all'istruzione è un diritto fondamentale anche per il pieno sviluppo della personalità, e la tutela dell'infanzia e la garanzia che tutti i minori possano godere in pienezza dei propri diritti deve essere il faro di uno Stato di diritto,

si chiede di sapere:

se il Ministro in indirizzo intenda effettuare una verifica rispetto agli ultimi dati relativi all'abbandono scolastico da parte delle bambine provenienti dalla comunità islamica;

se non intenda porre in essere iniziative mirate, anche di sensibilizzazione nei confronti della comunità islamica in Italia, al fine di circoscriverne l'entità;

quali iniziative intenda assumere per contrastare il fenomeno dell'abbandono dei percorsi di studio e formazione, garantendo a tutti i giovani il diritto all'istruzione.

(4-05898)

FAZZOLARI, BALBONI, CALANDRINI, GARNERO SANTANCHÈ, LA PIETRA, MALAN, RAUTI - *Al Presidente del Consiglio dei ministri e ai Ministri della salute e dell'economia e delle finanze*. - Premesso che:

dal febbraio 2020 ha avuto inizio la pandemia da SARS-COV2, che ha inciso sui tutti i settori dell'economia, delle imprese, del turismo, dei trasporti pubblici, della sanità, della scuola e dei servizi pubblici in generale, in maniera pervasiva ed esiziale;

la pandemia ha pesantemente segnato il mondo delle imprese italiane determinando a fine 2020, secondo i dati ISTAT, la chiusura di 73.000 imprese e la previsione di non riapertura per almeno altre 17.000; numeri impressionanti, che fotografano più di ogni analisi lo stato di estrema difficoltà in cui il nostro sistema imprenditoriale si è trovato nel giro di pochi mesi;

le misure di contenimento da COVID-19 hanno portato le aziende a ridurre drasticamente il personale in sede, rallentando tutti i settori produttivi con un danno, nel solo 2020, stimato in circa 150 mld di PIL, frutto appunto dell'impossibilità di frequentare il proprio posto di lavoro. In base al rapporto annuale sul mercato del lavoro 2020, frutto della collaborazione tra Ministero del lavoro e delle politiche sociali, ISTAT, INPS, INAIL e ANPAL, nella media dei primi tre trimestri del 2020 gli occupati sono diminuiti di 470.000 unità, nonostante il blocco dei licenziamenti deciso dal Governo;

il trasporto pubblico è stato fortemente penalizzato e, per quanto sia stato garantito il servizio pubblico essenziale, ancora oggi i mezzi di trasporto non risultano essere dotati di soluzioni idonee a ridurre il rischio di contagio, a meno che non si vogliano considerare tali le "raccomandazioni" sul distanziamento e sulla capienza ridotta;

anche le strutture ospedaliere pubbliche, nella prima fase pandemica veicolo principale di diffusione del contagio, sono carenti, ove non del tutto sprovviste, di dispositivi idonei alla sanificazione e sterilizzazione continua di superfici e ambienti;

analoghe carenze si riscontrano nelle scuole, dove l'assenza misure e dispositivi di sanificazione ha drammaticamente lasciato il posto alla didattica a distanza, con tutte le conseguenze negative che una simile approccio ha determinato negli studenti;

le spese di sanificazione e sterilizzazione, alle quali non si può certo rinunciare, costituiscono importanti voci di bilancio e impongono allo Stato (e ai privati) una programmazione e un impegno economico di medio lungo periodo;

considerato che:

la comunità scientifica mondiale negli ultimi 25 anni ha individuato, sperimentato e catalogato i raggi UV-C, classificandone l'efficacia battericida e virucida;

nel corso dei mesi di pandemia tutti i *test* di laboratorio effettuati su SARS-COV2, sottoposto a esposizione ai raggi UV-C, hanno ottenuto risultati positivi comprovando la totale inattivazione del *virus*, come anche dimostrato dagli studi dell'Istituto Nazionale di Astrofisica (INAF) e Università degli Studi di Milano, svolti in collaborazione con l'Istituto Nazionale dei Tumori di Milano (INT) e l'IRCCS Fondazione "Don Gnocchi" di Milano;

l'Istituto Superiore di Sanità, nel rapporto COVID-19 n. 25 del 2020, ha avallato quanto sostenuto dalla comunità scientifica in merito all'efficacia dei raggi UV-C su SARS-COV2;

a quanto risulta agli interroganti ad oggi, sul mercato, sono presenti dispositivi che danno la possibilità di utilizzare la tecnologia UV-C anche in presenza di persone e alimenti, garantendo una sanificazione degli ambienti costante e sicura;

risulta inoltre che numerose strutture ospedaliere, in diverse parti del mondo, abbiano sostituito i vecchi sistemi di sanificazione in favore di dispositivi a tecnologia UV-C, certificando e rendendo pubblico il risultato ottenuto, sia in termini di efficacia del prodotto, sia in termini di risparmio, grazie ai costi accessibili di tale tecnologia, fungendo anche da stimolo al suo utilizzo da parte di altri soggetti parimenti coinvolti in sanificazioni e sterilizzazioni;

la tecnologia in questione, proprio per le certificazioni ricevute e l'efficacia dimostrata, è in uso financo presso strutture militari come è il caso, ad esempio, del presidio Nato MSCOE - Modelling & Simulation Centre Of Excellence a Roma,

si chiede di sapere:

quali siano i motivi per i quali il Governo, nell'ambito della strategia di contenimento della pandemia, non abbia inserito e appositamente regolamentato l'utilizzo di dispositivi a tecnologia UV-C per la sanificazione di ospedali, mezzi di trasporto pubblico, scuole, pubblici uffici o altro, al fine di garantire la fruizione di ambienti pubblici a basso rischio di contagio;

se non ritenga opportuno impegnare risorse per lo sviluppo e la diffusione di dispositivi a tecnologia UV-C, sia al fine di garantire condizioni di maggior sicurezza, sia al fine di produrre un risparmio nel breve-medio termine per le casse dello Stato;

se non ritenga di promuovere e diffondere l'utilizzo di dispositivi a tecnologia UV-C, anche con l'emanazione di misure di incentivazione fiscale o di appositi bandi destinati alle imprese, con l'obiettivo di ridurre l'impatto del *virus* nei luoghi di lavoro, permettendo al contempo la ripresa delle attività in presenza;

quali siano i motivi e gli ostacoli per cui, anche a fronte di un utilizzo presso strutture sanitarie e militari di dispositivi a tecnologia UV-C e di un costo relativamente basso degli stessi, il Governo non intenda mettere a disposizione della comunità un simile strumento di protezione individuale e collettivo, di facile utilizzo e accesso.

(4-05899)

FERRARA - *Al Ministro della difesa*. - Premesso che:

il primo caporal maggiore David Tobini era un militare italiano deceduto in Afghanistan il 25 luglio 2011 durante l'operazione congiunta condotta

da forze italiane e afghane nella zona a nord-ovest della valle di Bala Murghab;

sua madre, Anna Rita Lo Mastro, ha chiesto da subito che venisse fatta chiarezza sulle cause della morte, evidenziando contraddizioni tra quanto veniva raccontato e quello che risultava negli atti acquisiti. Tra esse si annoveravano accertamenti mai eseguiti da parte del RIS, contraddizioni nella relazione autoptica e incongruenze nelle dichiarazioni rese dal teste oculare il caporal maggiore Luigi Russo;

il 2 agosto 2021 il giudice per le indagini preliminari ha archiviato il procedimento avendo rilevato l'intervenuta prescrizione del reato, seppur accogliendo le osservazioni evidenziate dalla squadra legale della famiglia del primo caporal maggiore Tobini;

nella sua ordinanza il giudice ha evidenziato un'incongruenza tra la posizione effettiva di Tobini rispetto a quanto riportato nel fascicolo di indagine e a quanto affermato dal testimone oculare Russo, in particolare ha individuato che la direzione del colpo che ha raggiunto Tobini è posteriore e non frontale come indicato dalla Procura, riscontrando altresì un'errata ricostruzione della traiettoria del colpo e della distanza da parte del reparto investigazioni scientifiche (RIS). Il giudice ha, infine, sottolineato che lo svolgimento di ulteriori indagini, come richiesto dalla parte offesa, tra cui *test* balistici mai effettuati, sarebbe stato utile e rilevante qualora intervenuto precedentemente alla prescrizione del reato;

considerato che:

in data 22 giugno 2021 sul quotidiano "Il Messaggero" è stata pubblicata una notizia, a firma del giornalista Mirko Polisano, che riportava quanto segue: "una lettera - scritta di pugno dal militare caduto a Bala Murghab nel luglio 2011 - sarebbe stata fatta sparire. A parlarne è stato proprio un soldato che avrebbe confidato ai colleghi di aver trovato la missiva e che 'fu consegnata' ma che 'non fu fatta mai recapitare'";

risulterebbe dagli atti che la missiva sarebbe stata inventariata come "lettera personale" il giorno 14 settembre 2011 dalla commissione nominata per predisporre l'elenco degli effetti di David Tobini da riconsegnare alla madre;

Anna Rita Lo Mastro aveva già segnalato che tale lettera, sebbene presente nell'elenco degli effetti personali del militare, non le era stata consegnata. Tuttavia, la possibilità che sia "stata fatta sparire" assumerebbe connotati di assoluta ed estrema gravità;

sulla questione è stata fatta, dall'avvocato difensore della parte offesa, una formale richiesta di accertamento al Ministero, affinché proceda a compiere tutte le relative indagini anche in virtù delle basilari norme inerenti all'obbligo di custodia facente capo al medesimo. Ad essa, però, non è mai stata data risposta,

si chiede di sapere:

se il Ministro in indirizzo sia a conoscenza dei fatti esposti;

quali siano i motivi per cui, durante gli anni in cui la madre di Tobini lamentava le incongruenze riscontrate nel fascicolo, non sono state svolte attività ispettive;

per quale ragione a David Tobini è stata consegnata la medaglia d'argento al valor militare anziché quella d'oro;

se, a seguito di quanto evidenziato dal giudice per le indagini preliminari, non ritenga avviare le opportune attività amministrative o ispettive nei confronti del caporal maggiore Luigi Russo relativamente alle incongruenze nelle sue dichiarazioni, di coloro che avrebbero ostacolato le indagini e di chi, responsabile della consegna della citata missiva, non ha provveduto a recapitarla alla madre.

(4-05900)

BARBARO - *Al Ministro dell'interno*. - Premesso che:

all'interrogante risulta che sia ormai insostenibile la mole di lavoro che gli operatori dell'Ufficio Immigrazione della Questura di Trapani sono costretti quotidianamente a sopportare; la situazione già di per sé gravosa, tipica del territorio siciliano, è vieppiù aggravata dalle nuove procedure antipandemiche: gli stranieri sbarcati a Pantelleria vengono, infatti, solitamente collocati presso i "C.A.S. Quarantena" di Valderice e di Marsala, centro quest'ultimo, peraltro, che fu chiuso a fine agosto 2020, dopo le gravi lesioni riportate dal personale della Polizia di Stato nel tentativo di arginare una fuga di massa, fenomeno purtroppo non occasionale e riguardante anche persone dichiarate positive al COVID-19 dalle Autorità sanitarie, tanto è che si è diffuso tra i residenti un senso di pericolo ed un diffuso allarme sociale, palesato anche con manifestazioni pubbliche;

la riapertura del C.P.R. di contrada Milo (con una capienza di oltre 200 stranieri) ha ulteriormente aggravato la situazione, tenuto conto che l'Ufficio Immigrazione di Trapani può contare su soli 12 operatori tra 3° e 4° Sezione, i quali hanno, giustamente, diritto alle giornate di aggiornamento professionale, alle giornate di addestramento, a fruire delle "assenze ordinarie", a fruire anche delle "assenze straordinarie" (all'esigenza) e soprattutto hanno il diritto di poter godere di tempo libero per un adeguato recupero psico-fisico;

a giudizio dell'interrogante occorre implementare l'organico in maniera stabile ed efficiente, non essendo più sufficiente ricorrere alle ore di lavoro straordinarie o ricorrere ad occasionali unità aggregate temporanee, tenuto conto della impossibilità di gestire numeri così impattanti di immigrati da trattenere nel periodo di quarantena,

si chiede di sapere:

se al Ministro in indirizzo risulti quante ore complessive di lavoro straordinario sono state effettuate, da inizio pandemia, dagli operatori di polizia della Questura di Trapani dell'Ufficio Immigrazione;

quanto personale aggregato ed aggiunto, anche civile, sia stato assegnato;

quando saranno consegnati i locali e gli ambienti ancora sottoposti a cantiere edilizio della struttura di Contrada Milo in Trapani;

per quale motivo gli stranieri non attendono la quarantena nelle apposite navi, ma sbarcano e vengono assegnati a strutture non idonee o comunque non destinate a ricovero sanitario;

come e se il Ministro in indirizzo intenda promuovere un'opera di rafforzamento strutturale di organico dell'Ufficio Immigrazione della Questura di Trapani.

(4-05901)

LANNUTTI, DI MICCO, ANGRISANI - *Al Presidente del Consiglio dei ministri e al Ministro dell'economia e delle finanze*. - Premesso che:

il 27 luglio 2021 il quotidiano "Domani" ha rivelato che il 49enne Simone Tabacci, figlio di Bruno Tabacci, attuale sottosegretario alla presidenza del Consiglio dei ministri, è stato assunto da Leonardo S.p.A., azienda italiana attiva nei settori della difesa, dell'aerospazio e della sicurezza, il cui maggiore azionista è il Ministero dell'economia e delle finanze, che possiede una quota di circa il 30 per cento. Il colosso ha assunto Simone Tabacci nella divisione *Chief strategic equity officier*, guidata da Giovanni Saccodato. La divisione si occupa del coordinamento delle partecipazioni e delle *joint venture* della società in mano al Ministero dell'economia e delle finanze e uno dei comparti chiave è l'aerospazio;

da qui l'incontrovertibile conflitto d'interessi: Tabacci padre, a quanto consta all'interrogante amico di vecchia data del presidente del Consiglio Draghi, ha tra le sue deleghe anche le politiche aerospaziali italiane, un settore considerato strategico per il nostro Paese, sia dal punto di vista economico (l'Italia ha raddoppiato i fondi stanziati per i programmi dell'Agenzia spaziale europea) che di geopolitica globale. Ma l'aerospazio è un settore fondamentale anche per Leonardo S.p.A.: Saccodato è anche presidente del Cda di Thales Alenia Space e vicepresidente di Mbda e Telespazio;

il quotidiano "Domani" scrive inoltre come la decisione di assumere il figlio del sottosegretario sia stata presa dall'amministratore delegato di Leonardo S.p.A., Alessandro Profumo;

considerato che il 15 ottobre 2020, la seconda sezione del Tribunale di Milano ha condannato Alessandro Profumo in qualità di ex presidente di Monte dei Paschi di Siena (MPS) a 6 anni di reclusione, 2,5 milioni di euro di sanzioni, 5 anni di interdizione dai pubblici uffici, 2 anni di interdizione

dagli uffici direttivi di imprese, per i reati di aggiotaggio e false comunicazioni sociali nella semestrale 2015. La stessa banca senese è stata condannata a una sanzione di 800.000 euro per la legge n. 231 del 2001 sulla responsabilità degli enti. In particolare, la condanna del Tribunale di Milano inflitta a Profumo per aggiotaggio e false comunicazioni sociali nella semestrale 2015 è dovuta alla contabilizzazione in bilancio dei derivati siglati con la giapponese Nomura. MPS ha infatti illecitamente contabilizzato come investimenti in titoli di Stato 5 miliardi di euro di temerarie speculazioni in prodotti finanziari derivati eseguiti con due banche estere (Deutsche Bank, Nomura), indicate anche come operazioni "Deutsche Bank" e "Nomura", con il fine (anch'esso risultato illecito) di occultare le perdite di altre operazioni di investimento denominate "Santorini" ed "Alexandria";

considerato inoltre che il 14 febbraio 2020 erano stati rinviati a giudizio per concorso in bancarotta fraudolenta 16 ex *manager* e funzionari di Unicredit, tra i quali Alessandro Profumo, imputato per il *crac* della società barese "Divania". È accusato, insieme agli altri 15 *manager* e funzionari, di aver ingannato il titolare dell'azienda, Francesco Saverio Parisi, in quanto sarebbe stato indotto a sottoscrivere 203 contratti con prodotti derivati che in pochi anni, secondo l'accusa, avrebbero portato la società al dissesto e al successivo fallimento. Il processo è iniziato il 5 maggio. Stando alle indagini, coordinate prima dall'ex pubblico ministero di Bari Isabella Ginefra e poi dal pubblico ministero Lanfranco Marazia, Unicredit, dopo avere convinto Parisi a sottoscrivere i contratti derivati assicurandogli che si trattava di un'operazione a costo zero, avrebbe invece distratto più di 183 milioni di euro dai conti correnti della società, senza autorizzazione del correntista, per portare a temine l'operazione. Tutto questo avrebbe contribuito al fallimento, nel 2011, dell'azienda di divani con sede nella zona industriale di Modugno (Bari), chiusa da allora con il licenziamento degli oltre 400 lavoratori;

considerato infine che il dottor Profumo ha ricevuto una liquidazione di 40 milioni di euro nel 2010 dalla banca Unicredit, considerata il doppio di quanto gli sarebbe spettato sulla base dei contratti siglati prima dell'uscita dall'istituto. Dopo la denuncia di Adusbef volta ad accertare se la buonuscita d'oro erogata da Unicredit a Profumo, la perizia del professor Stefano Loconte su incarico dei pubblici ministeri Nello Rossi e Michele Nardi della Procura di Roma sul fascicolo aperto a gennaio 2012, ha acclarato che quella maxi liquidazione nella corresponsione a Profumo di un incentivo all'esodo, "rappresentava un 'depauperamento patrimoniale' in danno della società e degli azionisti, che l'assegno di 40 milioni di euro non era congruo perché eccessivamente elevato di circa il doppio, e che tale condotta pur non integrando alcun reato (perciò la successiva archiviazione), potrebbe rilevare un illecito di natura civilistica, aprendo la strada al Cda di Unicredit di richiedere l'eccedenza di 20 milioni di euro, che il management di Unicredit si è ben guardata da richiedere procurando così un danno agli azionisti della banca,

si chiede di sapere:

se il Governo sia a conoscenza dei fatti descritti in premessa e se intenda esercitare i suoi poteri ispettivi per verificare le ragioni che hanno indotto MPS a fare quella scelta;

se non ritenga di dover promuovere le immediate dimissioni del dottor Profumo, per elementari ragioni di opportunità, dignità e senso dello Stato, alla luce della recente condanna per l'accertata falsificazione dei bilanci di MPS, avvenuta contabilizzando derivati come Titoli di Stato.

(4-05902)

Interrogazioni, da svolgere in Commissione

A norma dell'articolo 147 del Regolamento, le seguenti interrogazioni saranno svolte presso le Commissioni permanenti:

1ª Commissione permanente (Affari costituzionali, affari della Presidenza del Consiglio e dell'Interno, ordinamento generale dello Stato e della Pubblica Amministrazione):

3-02781 del senatore De Bertoldi ed altri, sugli scontri presso il cantiere TAV in Val di Susa;

9ª Commissione permanente (Agricoltura e produzione agroalimentare):

3-02771 del senatore Bergesio ed altri, sulle iniziative per incentivare la diffusione di modelli alimentari che abbiano al centro la dieta mediterranea;

3-02780 della senatrice Castellone, sulla propagazione della brucellosi bufalina in Campania;

12ª Commissione permanente (Igiene e sanità):

3-02769 della senatrice Fedeli ed altri, sulle difficoltà di prenotazione della vaccinazione da parte di soggetti non iscritti al SSN;

3-02770 della senatrice Fregolent, sull'effettuazione dei *test* salivari nelle scuole;

3-02775 della senatrice Boldrini, sulla cura dell'incontinenza;

3-02783 del senatore La Pietra ed altri, sul rilascio del *green pass* ai cittadini italiani residenti all'estero;

13ª Commissione permanente (Territorio, ambiente, beni ambientali):

3-02777 della senatrice La Mura, sul completamento della rete "Natura 2000" in Italia;

3-02778 della senatrice La Mura, sulla situazione di degrado e inquinamento del Rivo d'Arco, nel comune di Vico Equense (Napoli);

3-02779 della senatrice La Mura, sui piani per la pianificazione dello spazio marittimo.

Avviso di rettifica

Nel Resoconto stenografico della 353ª seduta pubblica del 29 luglio 2021:

a pagina 67, alla terza riga dell'intervento del senatore Augussori, sostituire le parole da: "Rinuncio al resto" fino a: "(*Applausi*)" con le seguenti: "Rinuncio a parte dei minuti che ho a disposizione e chiedo di poter mettere agli atti lo scritto del mio intervento con il quale dichiaro il voto favorevole del Gruppo Lega. (*Applausi*).

PRESIDENTE. La Presidenza l'autorizza in tal senso.";

a pagina 90, prima del titolo: "Testo integrale della dichiarazione di voto della senatrice Mantovani sul disegno di legge n. 2272", inserire il seguente intervento:

"**Dichiarazione di voto del senatore Augussori sul disegno di legge n. 2272**

Grazie Presidente, colleghi, vi prego di consentire anche a me di iniziare con parole non di circostanza ma di sincero ringraziamento: le rivolgo ai presidenti di Commissione Parrini ed Ostellari, ai relatori Valente e Caliendo, a tutti i commissari, alla sottosegretario ai rapporti con il Parlamento Caterina Bini e, soprattutto, a tutti gli eccellenti funzionari delle Commissioni e del Ministero della pubblica amministrazione. A voi tutti, grazie.

In questa settimana la nostra Aula è chiamata per la seconda volta ad approvare un decreto fondamentale per il futuro del nostro Paese.

Martedì abbiamo approvato il decreto semplificazioni ed oggi approviamo il decreto reclutamento. Entrambi sono determinanti per poter portare al successo l'ambizioso Piano Nazionale di Ripresa e Resilienza.

Volendo fare un paragone sportivo, visto che siamo anche in periodo di Giochi Olimpici, abbiamo una Ferrari da portare alla vittoria.

Per farlo abbiamo ingaggiato e messo alla guida il miglior pilota sulla piazza, il *premier* Mario Draghi, e abbiamo fatto il pieno di carburante, i 200 miliardi.

Le semplificazioni sono quindi i pneumatici che ci permettono di correre più veloce anche su un percorso accidentato e con questo decreto reclutamento aggiungiamo il motore... la forza lavoro ad alta prestazione che deve spingere la macchina facendole esprimere il meglio delle sue potenzialità.

Sono molteplici gli interventi presenti nel decreto emanato dal governo che permetteranno, sia nel settore tecnico delle pubbliche amministrazioni che nel campo della giustizia, di aumentare, migliorare ed efficientare le risorse umane che si occuperanno del PNRR.

Non avrei il tempo di illustrarli e commentarli tutti e me ne dimenticherei comunque qualcuno, quindi per non far torto ad alcuno non mi soffermerò sul testo base.

Evidenzio soltanto quella che per me è la più evidente delle innovazioni: non andremo più ad assumere ricercando i Tools, ma privilegiando le *Skills*.

Non assumeremo quindi ad esempio un ingegnere ed un informatico, ma un solo ingegnere con spiccate competenze informatiche.

Questo lo faremo dando fiducia ai giovani, alla generazione dei nativi digitali che proprio per le loro innate caratteristiche avranno la capacità di tirare questo Paese fuori dalle secche.

Crediamo in loro e glielo stiamo dimostrando con questo atto!

Voglio concentrarmi però sulle modifiche che introduciamo nel passaggio parlamentare, integrazioni che sono frutto del massiccio lavoro che abbiamo svolto in queste settimane in Commissione ed in particolare in questi ultimi intensi giorni.

Della parte relativa agli articoli che parlano di giustizia ha già detto tanto e bene il collega Emanuele Pellegrini, e visto che non saprei fare di meglio vi invito alla lettura del suo intervento.

Per quanto attiene alla prima parte del provvedimento la massima attenzione del gruppo Lega non poteva che essere dedicata alla tutela degli enti locali.

Ci ha molto spaventati la perplessità con cui ANCI ha accolto la norma che permetteva un'incontrollata mobilità in uscita dalle amministrazioni locali.

Stante la già presente carenza di personale in certe aree del Paese, il rischio di svuotamento dei Comuni avrebbe messo a serio rischio il funzionamento degli enti territoriali che anche non ne sono i titolari, di fatto dovranno "mettere a terra" le opere del PNRR.

Abbiamo chiesto con forza la deroga o il differimento come previsto per altri settori strategici, sanità istruzione e giustizia e abbiamo ottenuto un grande risultato: esenzione dalla revoca del nulla osta per i comuni con meno di cento dipendenti e per gli altri l'introduzione di criteri talmente rigidi e complessi che di fatto si tradurranno nel mantenimento del regime attuale.

Siamo poi intervenuti sulla delicata situazione dei segretari comunali: il Gruppo Lega ha proposto e visto approvare sia la proroga della funzione dei vicesegretari per altri dodici mesi sia la copertura del 100 per cento del *turn over* rispetto all'anno precedente.

Due soluzioni sì tampone, ma fondamentali per disinnescare quello che è un vero e proprio collo di bottiglia, come ben vi ha ben spiegato oggi(ieri) il sindaco di Misano Gera D'Adda, nonché senatrice Daisy Pirovano, almeno finché non verrà trovata una soluzione per accelerare l'immissione in ruolo di nuovi segretari comunali e provinciali.

Siamo soddisfatti per il risultato e continueremo a lavorare su ogni provvedimento nell'interesse dei comuni in particolare quelli medio piccoli.

Ci dispiace però che in questo parlamento vi sia una consistente forza politica che non perde occasione per creare difficoltà ai comuni proponendo al più soluzioni fantasiose ed utopistiche ma che mal si conciliano con la realtà e le difficoltà che si vivono quotidianamente tra le mura degli uffici comunali e che ogni giorno mettono alla prova sindaci assessori e consiglieri comunali.

Comprendiamo che chi non ha potuto maturare l'esperienza da amministratore, nemmeno di un condominio, faccia fatica a confrontarsi con questi temi, ma proprio per questo dovrebbe astenersene piuttosto che continuare a fare danno.

Confidando che questo atteggiamento sia limitato a pochi senatori e senatrici voglio ricordare una frase del noto scienziato Stephen Hawking "il più grande nemico della conoscenza non è l'ignoranza, è l'illusione della conoscenza"

Infine un solo breve cenno ad un nostro piccolo emendamento che però mi sta particolarmente a cuore, quello che prevede nei nuovi concorsi di utilizzare gli strumenti compensativi di cui necessitano i soggetti portatori di DSA. È un piccolo gesto, ma è la dimostrazione che la Lega, davvero, non lascia indietro nessuno.

Concludo Presidente, annunciando il voto favorevole del Gruppo Lega al provvedimento così come migliorato dal Senato e il voto favorevole alla fiducia a questo Governo. In entrambi il forte impatto delle proposte della Lega è evidente e questo è un bene per il Paese."