292. **Allegato A**

DOCUMENTI ESAMINATI NEL CORSO DELLA SEDUTA

COMUNICAZIONI ALL'ASSEMBLEA

INDICE

N. B. Questo allegato reca i documenti esaminati nel corso della seduta e le comunicazioni all'Assemblea non lette in aula.

ORGANIZZAZIONE DEI TEMPI DI ESAME: PDL N. 1276

PDL N. 1276 - MODIFICA DELL'ARTICOLO 2407 DEL CODICE CIVILE, IN MATERIA DI RESPONSABILITÀ DEI COMPONENTI DEL COLLEGIO SINDACALE

Tempo complessivo: 13 ore, di cui:

- discussione sulle linee generali: 8 ore;
- seguito dell'esame: 5 ore.

	Discussione generale	*Seguito dell'esame*
Relatore	**20 minuti**	**20 minuti**
Governo	**20 minuti**	**20 minuti**
Richiami al Regolamento	**10 minuti**	**10 minuti**
Tempi tecnici		**15 minuti**
Interventi a titolo personale	**1 ora e 20 minuti**	**45 minuti** *(con il limite massimo di 5 minuti per il complesso degli interventi di ciascun deputato)*
Gruppi	**5 ore e 50 minuti**	**3 ore e 10 minuti**
Fratelli d'Italia	***45 minuti***	***37 minuti***
Partito Democratico – Italia democratica e progressista	***39 minuti***	***26 minuti***
Lega – Salvini premier	***38 minuti***	***25 minuti***
MoVimento 5 Stelle	***36 minuti***	***22 minuti***
Forza Italia – Berlusconi presidente – PPE	***36 minuti***	***20 minuti***
Azione – Popolari Europeisti Riformatori – Renew Europe	***32 minuti***	***13 minuti***
Alleanza Verdi e Sinistra	***31 minuti***	***12 minuti***
Noi Moderati (Noi Con L'Italia, Coraggio Italia, Udc e Italia al Centro) – MAIE	***31 minuti***	***12 minuti***
Italia Viva – Il Centro – Renew Europe	***31 minuti***	***12 minuti***
Misto:	***31 minuti***	***11 minuti***
Minoranze Linguistiche	*18 minuti*	*6 minuti*
+Europa	*13 minuti*	*5 minuti*

COMUNICAZIONI

Missioni valevoli nella seduta del 14 maggio 2024.

Albano, Ascani, Barbagallo, Barelli, Battistoni, Bellucci, Benvenuto, Bignami, Bitonci, Braga, Brambilla, Calderone, Cappellacci, Carfagna, Carloni, Casasco, Cavandoli, Cecchetti, Centemero, Cesa, Cirielli, Colosimo, Enrico Costa, Sergio Costa, Deidda, Della Vedova, Delmastro Delle Vedove, Donzelli, Faraone, Fassino, Ferrante, Ferro, Fitto, Foti, Frassinetti, Freni, Gardini, Gava, Gebhard, Gemmato, Giglio Vigna, Giorgetti, Gribaudo, Guerini, Gusmeroli, Leo, Letta, Lollobrigida, Lupi, Magi, Mangialavori, Maschio, Mazzi, Meloni, Minardo, Molinari, Mollicone, Molteni, Mulè, Nordio, Osnato, Nazario Pagano, Patriarca, Pellegrini, Pichetto Fratin, Prisco, Rampelli, Richetti, Rixi, Rizzetto, Roccella, Romano, Rosato, Angelo Rossi, Rotelli, Scerra, Schullian, Semenzato, Francesco Silvestri, Siracusano, Sportiello, Stefani, Sudano, Tabacci, Tajani, Trancassini, Traversi, Tremonti, Vaccari, Varchi, Vinci, Zaratti, Zoffili, Zucconi.

(Alla ripresa pomeridiana della seduta).

Albano, Ascani, Barbagallo, Barelli, Battistoni, Bellucci, Benvenuto, Bignami, Bitonci, Braga, Brambilla, Calderone, Cappellacci, Carfagna, Carloni, Casasco, Cavandoli, Cecchetti, Centemero, Cesa, Cirielli, Colosimo, Enrico Costa, Sergio Costa, Deidda, Della Vedova, Delmastro Delle Vedove, Donzelli, Faraone, Fassino, Ferrante, Ferro, Fitto, Foti, Frassinetti, Freni, Gardini, Gava, Gebhard, Gemmato, Giglio Vigna, Giorgetti, Gribaudo, Guerini, Gusmeroli, Leo, Letta, Lollobrigida, Lupi, Magi, Mangialavori, Maschio, Mazzi, Meloni, Minardo, Molinari, Mollicone, Molteni, Morrone, Mulè, Nordio, Osnato, Nazario Pagano, Patriarca, Pellegrini, Pichetto Fratin, Prisco, Rampelli, Richetti, Rixi, Rizzetto, Roccella, Romano, Rosato, Angelo Rossi, Rotelli, Scerra, Schullian, Semenzato, Francesco Silvestri, Siracusano, Sportiello, Stefani, Sudano, Tabacci, Tajani, Trancassini, Traversi, Tremonti, Vaccari, Varchi, Vinci, Zaratti, Zoffili, Zucconi.

Annunzio di proposte di legge.

In data 13 maggio 2024 sono state presentate alla Presidenza le seguenti proposte di legge d'iniziativa dei deputati:

MADIA: « Disposizioni concernenti l'obbligo di verifica dell'età degli utenti dei servizi della società dell'informazione, la disciplina dei proventi derivanti dalla diffusione di immagini di minori attraverso le piattaforme telematiche nonché l'accesso al numero telefonico di emergenza per l'infanzia » (1863);

CONTE ed altri: « Modifica dell'articolo 5-*bis* della legge 24 gennaio 1979, n. 18, in materia di incompatibilità e incandidabilità dei deputati, dei senatori e dei componenti del Governo alla carica di membro del Parlamento europeo » (1864);

ZANELLA ed altri: « Disposizioni per il finanziamento del fabbisogno sanitario nazionale *standard* cui concorre lo Stato, il potenziamento dell'assistenza territoriale e

la riduzione delle liste di attesa delle prestazioni sanitarie » (1865).

Saranno stampate e distribuite.

Annunzio di disegni di legge.

In data 13 maggio 2024 è stato presentato alla Presidenza il seguente disegno di legge:

dai Ministri per la famiglia, la natalità e le pari opportunità e della giustizia:

« Disposizioni in materia di tutela dei minori in affidamento » (1866).

Sarà stampato e distribuito.

Assegnazione di progetti di legge a Commissioni in sede referente.

A norma del comma 1 dell'articolo 72 del Regolamento, i seguenti progetti di legge sono assegnati, in sede referente, alle sottoindicate Commissioni permanenti:

III Commissione (Affari esteri)

« Ratifica ed esecuzione della Convenzione tra il Governo della Repubblica italiana e il Governo del Principato del Liechtenstein per eliminare le doppie imposizioni in materia di imposte sul reddito e per prevenire l'evasione e l'elusione fiscale, con Protocollo e Protocollo Aggiuntivo sull'Arbitrato, fatta a Roma e Vaduz il 12 luglio 2023 » (1847) *Parere delle Commissioni I, II, V, VI e XIV.*

VIII Commissione (Ambiente)

SERGIO COSTA ed altri: « Modifica all'articolo 36 della legge 6 dicembre 1991, n. 394, in materia di istituzione dell'area marina protetta del golfo di Napoli » (1537) *Parere delle Commissioni I, V e della Commissione parlamentare per le questioni regionali;*

BARABOTTI ed altri: « Modifiche all'articolo 31 della legge 23 dicembre 1998, n. 448, in materia di corrispettivi per la cessione in proprietà di alloggi di edilizia residenziale pubblica » (1678) *Parere delle Commissioni I, II, V, VI e della Commissione parlamentare per le questioni regionali.*

X Commissione (Attività produttive)

SERGIO COSTA: « Modifica all'articolo 7 del decreto legislativo 4 luglio 2014, n. 102, in materia di interventi in favore delle famiglie che versano in condizioni di povertà energetica » (1599) *Parere delle Commissioni I, V, VIII, XII, XIV e della Commissione parlamentare per le questioni regionali.*

XII Commissione (Affari sociali)

MARROCCO: « Disposizioni per l'istituzione, il potenziamento e l'integrazione dei servizi di psiconcologia nell'ambito del percorso di assistenza e di cura dei pazienti oncologici e oncoematologici » (1637) *Parere delle Commissioni I, V, XI e della Commissione parlamentare per le questioni regionali;*

CIOCCHETTI ed altri: « Modifica del comma 255 dell'articolo 1 della legge 27 dicembre 2017, n. 205, e altre disposizioni nonché delega al Governo per il riconoscimento e la tutela della figura del *caregiver* familiare » (1690) *Parere delle Commissioni I, II, V, X, XI, XIV e della Commissione parlamentare per le questioni regionali.*

Annunzio di sentenze della Corte costituzionale.

La Corte costituzionale ha trasmesso, ai sensi dell'articolo 30, secondo comma, della legge 11 marzo 1953, n. 87, copia delle seguenti sentenze che, ai sensi dell'articolo 108, comma 1, del Regolamento, sono inviate alle sottoindicate Commissioni competenti per materia, nonché alla I Commissione (Affari costituzionali):

in data 13 maggio 2024 Sentenza n. 85 del 16 aprile – 13 maggio 2024 (Doc. VII, n. 322),

con la quale:

dichiara l'illegittimità costituzionale dell'articolo 2-*quinquies*, comma 1, del de-

creto-legge 30 aprile 2020, n. 28 (Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19), convertito, con modificazioni, nella legge 25 giugno 2020, n. 70, nella parte in cui non prevede, al terzo periodo, dopo le parole « Quando si tratta di detenuti o internati per uno dei delitti previsti dal primo periodo del comma 1 dell'articolo 4-bis della legge 26 luglio 1975, n. 354, », le parole « per i quali si applichi il divieto dei benefici ivi previsto, »:

alla II Commissione (Giustizia);

in data 13 maggio 2024 Sentenza n. 86 del 16 aprile – 13 maggio 2024 (Doc. VII, n. 323),

con la quale:

dichiara l'illegittimità costituzionale dell'articolo 628, secondo comma, del codice penale, nella parte in cui non prevede che la pena da esso comminata è diminuita in misura non eccedente un terzo quando per la natura, la specie, i mezzi, le modalità o circostanze dell'azione, ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità;

dichiara, in via consequenziale, ai sensi dell'articolo 27 della legge 11 marzo 1953, n. 87 (Norme sulla costituzione e sul funzionamento della Corte costituzionale), l'illegittimità costituzionale dell'articolo 628, primo comma, del codice penale, nella parte in cui non prevede che la pena da esso comminata è diminuita in misura non eccedente un terzo quando per la natura, la specie, i mezzi, le modalità o circostanze dell'azione, ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità:

alla II Commissione (Giustizia);

in data 14 maggio 2024 Sentenza n. 87 del 20 marzo – 14 maggio 2024 (Doc. VII, n. 324),

con la quale:

dichiara l'illegittimità costituzionale dell'articolo 8 della legge della Regione Piemonte 24 aprile 2023, n. 6 (Bilancio di previsione finanziario 2023-2025), nella parte in cui, nel sostituire il comma 2 dell'articolo 14 della legge Regione Piemonte 5 dicembre 2016, n. 24 (Assestamento del bilancio di previsione finanziario 2016-2018 e disposizioni finanziarie), ha stabilito che « 2. A decorrere dall'esercizio 2023 e fino all'esercizio 2032 è garantito il trasferimento di cassa in favore della gestione sanitaria da prelevare dal conto di tesoreria della gestione ordinaria, per importi, riferiti a ciascun anno, pari a 93.000.000,00 negli esercizi dal 2023 al 2025 e a euro 92.000.000,00 negli esercizi dal 2026 al 2032, da destinare alla riduzione dei residui passivi verso le aziende sanitarie regionali al 31 dicembre 2015. », invece che « 2. A decorrere dall'esercizio 2023 e fino all'esercizio 2026 è garantito il trasferimento di cassa in favore della gestione sanitaria da prelevare dal conto di tesoreria della gestione ordinaria, di un importo complessivo pari a 923 milioni di euro, da destinare alla riduzione dei residui passivi verso le aziende sanitarie regionali al 31 dicembre 2015 », secondo modalità rimesse a successiva legge regionale:

alla XII Commissione (Affari sociali).

La Corte costituzionale ha depositato in cancelleria la seguente sentenza che, ai sensi dell'articolo 108, comma 1, del Regolamento, è inviata alla II Commissione (Giustizia) nonché alla I Commissione (Affari costituzionali):

Sentenza n. 88 del 16 aprile – 14 maggio 2024(Doc. VII, n. 325),

con la quale:

dichiara inammissibile la questione di legittimità costituzionale dell'articolo 1, comma 1, del decreto legislativo 15 gennaio 2016, n. 7 (Disposizioni in materia di abro-

gazione di reati e introduzione di illeciti con sanzioni pecuniarie civili, a norma dell'articolo 2, comma 3, della legge 28 aprile 2014, n. 67), sollevata, in riferimento all'articolo 76 della Costituzione, dal Tribunale ordinario di Firenze, sezione prima penale;

dichiara non fondata la questione di legittimità costituzionale dell'articolo 1, comma 4, del decreto legislativo 15 gennaio 2016, n. 8 (Disposizioni in materia di depenalizzazione, a norma dell'articolo 2, comma 2, della legge 28 aprile 2014, n. 67), sollevata, in riferimento all'articolo 76 della Costituzione, dal Tribunale ordinario di Firenze, sezione prima penale.

Trasmissione dalla Corte dei conti.

Il Presidente della Corte dei conti, con lettera in data 14 maggio 2024, ha trasmesso, ai sensi dell'articolo 7, comma 7, del decreto-legge 31 maggio 2021, n. 77, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108, la relazione della Corte dei conti sullo stato di attuazione del Piano nazionale di ripresa e resilienza (PNRR), aggiornata al 13 marzo 2024 (Doc. XIII-*bis*, n. 3).

Questa relazione è trasmessa alla V Commissione (Bilancio), nonché a tutte le altre Commissioni permanenti.

Il Presidente della Sezione centrale di controllo sulla gestione delle Amministrazioni dello Stato della Corte dei conti, con lettera in data 14 maggio 2024, ha trasmesso, ai sensi dell'articolo 3, comma 6, della legge 14 gennaio 1994, n. 20, la deliberazione n. 62/2024 del 17 aprile-13 maggio 2024, con la quale la Sezione stessa ha approvato il rapporto avente a oggetto « Segnalazioni inviate alla Corte dei conti dagli OIV e istituti di premialità riconosciuti al personale dipendente (2020-2022) ».

Questo documento è trasmesso alla I Commissione (Affari costituzionali), alla V Commissione (Bilancio) e alla XI Commissione (Lavoro).

Trasmissione dal Dipartimento per gli affari europei della Presidenza del Consiglio dei ministri.

Il Dipartimento per gli affari europei della Presidenza del Consiglio dei ministri, con lettera in data 13 maggio 2024, ha trasmesso la seguente relazione concernente il seguito dato dal Governo agli indirizzi definiti dalle Camere in merito a progetti di atti dell'Unione europea o ad atti preordinati alla formulazione degli stessi:

relazione, predisposta dal Ministero delle imprese e del *made in Italy*, concernente il seguito del documento della 9ª Commissione (Industria) del Senato (atto Senato Doc XVIII, n. 4) in merito alla proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro atto a garantire un approvvigionamento sicuro e sostenibile di materie prime critiche e che modifica i regolamenti (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1724 e (UE) 2019/1020 (COM(2023) 160 final) (COM(2023) 192 final) e alla comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni – Un approvvigionamento sicuro e sostenibile di materie prime critiche a sostegno della duplice transizione (COM(2023) 165 final).

Questa relazione è trasmessa alla X Commissione (Attività produttive) e alla XIV Commissione (Politiche dell'Unione europea).

Trasmissione dalla Regione autonoma della Sardegna.

La Regione autonoma della Sardegna, con lettera in data 13 maggio 2024, ha trasmesso, ai sensi dell'articolo 2, comma 5, della legge regionale 7 ottobre 2005, n. 13, il decreto della Presidente della Regione di scioglimento del consiglio comunale di Goni.

Questa documentazione è depositata presso il Servizio per i Testi normativi a disposizione degli onorevoli deputati.

Richiesta di parere parlamentare su atti del Governo.

Il Ministro per i rapporti con il Parlamento, con lettera in data 9 maggio 2024, ha trasmesso, ai sensi degli articoli 1 e 10 della legge 21 febbraio 2024, n. 15, la richiesta di parere parlamentare sullo schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale all'articolo 138 del regolamento (UE) 2018/1139 e alla direttiva (UE) 2022/2380, che modificano la direttiva 2014/53/UE, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio **(155)**.

Questa richiesta è assegnata, ai sensi del comma 4 dell'articolo 143 del Regolamento, alla IX Commissione (Trasporti) nonché, ai sensi del comma 2 dell'articolo 126 del Regolamento, alla XIV Commissione (Politiche dell'Unione europea), che dovranno esprimere i prescritti pareri entro il 23 giugno 2024. È altresì assegnata, ai sensi del comma 2 dell'articolo 96-*ter* del Regolamento, alla V Commissione (Bilancio), che dovrà esprimere i propri rilievi sulle conseguenze di carattere finanziario entro il 3 giugno 2024.

Atti di controllo e di indirizzo.

Gli atti di controllo e di indirizzo presentati sono pubblicati nell'*Allegato B* al resoconto della seduta odierna.

INTERPELLANZA E INTERROGAZIONI

Iniziative di competenza volte a rendere definitivo il trasferimento dell'archivio processuale relativo al disastro del Vajont presso la sede dell'Archivio di Stato di Belluno – 3-01194

A) Interrogazione

SCARPA e FASSINO. — *Al Ministro della cultura.* — Per sapere – premesso che:

l'articolo 30 del decreto legislativo 22 gennaio 2004, n. 42 (Codice dei beni culturali e del paesaggio), stabilisce che lo Stato, le regioni, gli altri enti pubblici territoriali nonché ogni altro ente e istituto pubblico hanno l'obbligo di garantire la sicurezza e la conservazione dei beni culturali di loro appartenenza e, al comma 4, statuisce che i medesimi soggetti hanno l'obbligo di conservare i propri archivi nella loro organicità e di ordinarli. I soggetti medesimi hanno altresì l'obbligo di inventariare i propri archivi storici, costituiti dai documenti relativi agli affari esauriti da oltre quaranta anni e istituiti in sezioni separate;

l'articolo 41, comma 1, primo capoverso, del predetto decreto legislativo, stabilisce che gli organi giudiziari e amministrativi dello Stato versano all'archivio centrale dello Stato e agli archivi di Stato i documenti relativi agli affari esauriti da oltre quarant'anni, unitamente agli strumenti che ne garantiscono la consultazione;

nel contesto normativo sopra delineato si inserisce l'intervenuto spostamento dall'archivio di Stato dell'Aquila a quello di Belluno del fondo archivio processuale del Vajont, deposito temporaneo avvenuto nel 2009 in conseguenza del terremoto che colpì il capoluogo abruzzese;

il predetto fondo è nella titolarità dell'archivio di Stato dell'Aquila, territorialmente competente in virtù dell'avvenuta celebrazione del processo di secondo grado presso la corte di appello dell'Aquila;

allo stato attuale, il deposito temporaneo nell'archivio di Stato di Belluno non è stato formalmente rinnovato, mentre la direzione dell'archivio di Stato dell'Aquila ha già attivato la procedura per la restituzione del fondo Vajont in base al principio della titolarità;

da alcuni anni è in corso il progetto di riproduzione digitale di tutto il fascicolo processuale del Vajont e ciò sulla scorta della convenzione stipulata nel dicembre 2009 tra la direzione generale per gli archivi, la fondazione Vajont, gli archivi di Stato di Belluno e L'Aquila, i comuni di Longarone e di Castellavazzo e dovrebbe concludersi, attraverso nuovi finanziamenti ministeriali, con l'immissione in rete dei documenti, lavoro per il quale saranno tuttavia necessari continui riscontri sulla documentazione cartacea: è dunque del tutto evidente che l'ipotesi di un trasferimento della documentazione *in itinere* non può che risolversi con effetti a detrimento dei lavori necessari alla conclusione del progetto;

è stata avviata la procedura per candidare l'archivio processuale del disastro della diga del Vajont all'iscrizione nel registro della memoria dell'Unesco, conclusasi proprio nel 2023 con il suo inserimento;

si ritiene che il mantenimento del fondo archivio processuale Vajont presso l'attuale sede dell'archivio di Stato di Belluno costituirebbe altresì una sorta di riconoscimento etico per le popolazioni colpite direttamente dalla tragedia –:

se il Ministro interrogato non intenda adottare iniziative di competenza volte a rendere definitivo il trasferimento del suddetto fondo di archivio processuale presso la sede dell'archivio di Stato di Belluno.

(3-01194)

Iniziative di competenza in sede europea volte a contrastare la produzione di* foie gras *attraverso l'alimentazione forzata, con particolare riferimento all'eliminazione del requisito dei pesi minimi del fegato di anatre e oche di cui al regolamento (CE) n. 543 del 2008 – 2-00372; 3-01195; 3-01196

B) Interpellanza e interrogazioni

I sottoscritti chiedono di interpellare il Ministro dell'agricoltura, della sovranità alimentare e delle foreste, per sapere – premesso che:

il *foie gras*, letteralmente fegato grasso, è un piatto tipico della cucina francese a base di fegato d'oca o d'anatra ed è considerato ancora in diverse parti del mondo una prelibatezza;

la produzione di *foie gras*, tuttavia, avviene nella maggior parte dei casi attraverso l'alimentazione forzata delle oche e delle anatre, utilizzando un trattamento denominato *gavage*, che permette nel minor tempo possibile di ingrassare il fegato degli animali;

tale tecnica prevede che ai volatili venga somministrato con forza più cibo di quanto assumerebbero in natura, o volontariamente negli allevamenti domestici, attraverso un imbuto equipaggiato da un lungo tubo di metallo di 20-30 centimetri che immette il cibo direttamente nell'esofago dell'animale;

l'alimentazione consiste solitamente in grano bollito nel grasso per facilitarne l'ingestione e provocare grandi depositi di lipidi nel fegato, ottenendo così una consistenza gelatinosa che tanto è ricercata in gastronomia;

l'inserimento e l'estrazione del tubo danneggiano le pareti della gola e dell'esofago degli animali, provocando irritazioni e ferite ed esponendo oche e anatre al rischio costante di infezioni. Inoltre, durante la pratica dell'ingrassamento forzato, l'animale cerca di divincolarsi rischiando fratture del collo e perforazione dell'esofago e di conseguenza la morte. Durante tale pratica, non di rado, gli animali muoiono anche soffocati dal proprio vomito. In generale sembrerebbe che la mortalità in questi allevamenti sia fino a 10 volte superiore rispetto agli allevamenti in cui non si pratica il « *force-feeding* »;

il *gavage* è subito per lo più da anatre e oche di sesso maschile, poiché generalmente le femmine vengono uccise appena nate a causa del loro fegato considerato di qualità inferiore;

alla fine della fase di ingozzamento (l'ultima fase di allevamento per il *foie gras* in cui anatre e oche vengono alimentate forzatamente due volte al giorno per 15 giorni) il fegato di ogni animale può essere fino a dieci volte più grande di quello di un animale che non ha subito questo trattamento, tanto da arrivare ad uno stato di steatosi epatica – patologia legata a un enorme accumulo di grasso;

in Italia, dall'entrata in vigore del decreto legislativo 26 marzo 2001, n. 146, recante « Attuazione della direttiva 98/58/CE relativa alla protezione degli animali negli allevamenti », è vietata la produzione di « fegato grasso » di oche e anatre mediante alimentazione forzata. Tuttavia il *foie gras* tramite alimentazione forzata viene ancora prodotto in cinque dei 27 Stati dell'Unione europea: Francia, Ungheria, Bulgaria, Spagna e Belgio (solo nella Vallonia), che lo producono e lo esportano a livello globale; la Francia da sola produce circa l'80 per cento del *foie gras* consumato ed esportato in tutto il mondo;

in Italia il consumo della particolarità culinaria è solo l'1 per cento rispetto al consumo della Francia; tuttavia, anche gli stessi francesi hanno contestato l'alimentazione forzata, ammessa, all'interno dell'Unione europea, in Francia, Ungheria, Bulgaria, Spagna e Belgio;

in alcuni Paesi terzi, quali India, Regno Unito, Argentina e Stati Uniti, oltre alla produzione sono vietati anche il consumo e la vendita di *foie gras* prodotto attraverso l'alimentazione forzata;

in Europa, il requisito dei pesi minimi del fegato di anatre e oche, attualmente previsto dal regolamento (CE) n. 543 del 2008 relativo alle norme di commercializzazione per le carni di pollame, ad avviso degli interpellanti, non ha alcuna base scientifica o tradizionale e, di fatto, impedisce la produzione di *foie gras* senza ricorrere al *gavage*;

il tema è già da tempo all'attenzione della Commissione europea (Direzione generale agricoltura e sviluppo rurale) che, nell'ambito della revisione delle norme sulla commercializzazione per la carne di pollame, ad aprile 2023 ha lanciato una consultazione pubblica, vedendo arrivare 2245 *input* da parte di cittadini, operatori commerciali e associazioni. Il 90 per cento di questi chiede l'eliminazione del requisito dei pesi minimi del fegato, per permettere ai consumatori di scegliere *foie gras* prodotto senza alimentazione forzata;

il 30 giugno 2023 presso il Parlamento europeo è stata presentata un'interrogazione scritta, firmata da ben 84 parlamentari europei, 15 di questi italiani e appartenenti ad ogni schieramento politico, atta a richiedere l'eliminazione del requisito dei pesi minimi del fegato di anatre e oche e, quindi, a permettere la produzione di *foie gras* senza *gavage*;

il nostro Paese, attraverso le azioni di precedenti Governi, si è più volte fatto portavoce in Europa di questa causa, schierandosi ufficialmente contro il requisito dei pesi minimi del fegato e a tutela del benessere animale;

è bene ricordare che nell'ambito della strategia *Farm to Fork*, che si colloca al centro del *Green deal* europeo, un punto cruciale consiste nella tutela del benessere degli animali, per cui la Commissione europea si era impegnata a rivedere la legislazione sull'etichettatura dei prodotti alimentari, sulle condizioni degli animali negli allevamenti, durante il trasporto e nel momento dell'abbattimento entro l'anno 2023; tale revisione non è stata tuttavia portata a termine –:

se, alla luce di quanto esposto in premessa, non intenda intervenire nelle competenti sedi europee al fine di sostenere la causa dell'eliminazione del requisito dei pesi minimi di fegato di anatre e di oche, allo scopo di porre fine ad una pratica crudele e contraria a qualsiasi concetto di benessere animale, contribuendo ad abolire il maltrattamento degli animali, sottoposti a inutili sofferenze e promuovendo *standard* di allevamento già praticati dagli allevatori italiani.

(2-00372) « Cherchi, Caramiello, Sergio Costa, Di Lauro, Morfino, Quartini, Marianna Ricciardi, Amato, Baldino, Carmina, Ilaria Fontana, Fede, Scutellà, Torto, Cappelletti, Caso, Iaria, Ferrara, Dell'Olio, D'Orso, Scerra ».

VACCARI, MARINO, FORATTINI e ANDREA ROSSI. — *Al Ministro dell'agricoltura, della sovranità alimentare e delle foreste, al Ministro per gli affari europei, il Sud, le politiche di coesione e il PNRR.* — Per sapere – premesso che:

la produzione di *foie gras* tramite alimentazione forzata in Italia è vietata dal 2001, ma avviene ancora in cinque dei 27 Stati dell'Unione europea: Francia, Ungheria, Bulgaria, Spagna e Belgio (solo nella Vallonia). Si tratta di un prodotto di nicchia venduto ancora oggi in Europa e nel nostro Paese, che provoca la sofferenza estrema di milioni di animali in Europa, dove vengono prodotte più di 19 mila tonnellate di *foie gras*, circa il 90 per cento della produzione globale;

attualmente, il regolamento (CE) n. 543 del 2008 relativo alle norme di commercializzazione per le carni di pollame prevede che, per produrre *foie gras*, il fegato di un'anatra debba pesare almeno 300 grammi e quello di un'oca almeno 400. Ma si tratta di pesi che questi animali non raggiungono in natura e che è possibile realizzare a livello industriale solo attraverso l'alimentazione forzata, come stabilito nel 1991 dalla Commissione europea. Tale requisito sui pesi minimi non ha alcuna base scientifica o tradizionale. La stessa produzione di *foie gras* è stata fortemente condannata da un rapporto del Comitato scientifico veterinario dell'Unione europea, che giudica l'alimentazione forzata « nociva per il benessere degli animali ». Tuttavia, nonostante anche la Fao ritenga la pratica dell'alimentazione forzata nociva per gli animali, nel 2022 il Parlamento europeo ha approvato una relazione in cui si afferma che questa produzione è basata su procedure di allevamento rispettose dei criteri di benessere animale;

l'Unione europea continua a permettere che una pratica così atroce venga perpetrata nei confronti di milioni di animali allevati –:

quali iniziative intendano intraprendere nelle sedi europee al fine di avviare in tempi brevi l'*iter* per l'eliminazione del requisito dei pesi minimi del fegato di anatre e oche di cui al regolamento (CE) n. 543 del 2008, nonché al fine di tutelare i produttori che non utilizzano alimentazione forzata e, per questo, fortemente penalizzati. (3-01195)

ZANELLA e DORI. — *Al Ministro dell'agricoltura, della sovranità alimentare e delle foreste, al Ministro per gli affari europei, il Sud, le politiche di coesione e il PNRR*. — Per sapere – premesso che:

con il decreto legislativo n. 146 del 2001, recante « Attuazione della direttiva 98/58/CE relativa alla protezione degli animali negli allevamenti », è stata vietata nel nostro Paese la produzione di « fegato grasso » di oche e anatre mediante alimentazione forzata (o *gavage*), che consiste nell'inserire un tubo nella gola degli animali, costringendoli a ingurgitare in pochi secondi e per più volte al giorno una quantità eccessiva di cibo;

tuttavia, nell'Unione europea il *foie gras* tramite alimentazione forzata viene ancora prodotto in Francia, Ungheria, Bulgaria, Spagna e Belgio (solo nella Vallonia);

durante tale pratica, non di rado, gli animali subiscono gravi lesioni o muoiono soffocati dal proprio vomito;

l'obiettivo dell'allevatore è ingrassare il fegato dell'animale al punto di arrivare ad indurre la « steatosi epatica », una vera e propria patologia del fegato, che poi viene immesso sul mercato col nome di *foie gras*;

il requisito dei pesi minimi del fegato di anatre e oche, attualmente previsto dal regolamento (CE) n. 543 del 2008 relativo alle norme di commercializzazione per le carni di pollame, non ha alcuna base scientifica o tradizionale e, di fatto, impedisce la produzione di *foie gras* senza ricorrere al *gavage* o alimentazione forzata;

Animal Equality e numerose altre associazioni animaliste da sempre si battono con forza per il rispetto del benessere animale e contro il requisito dei pesi minimi del fegato di anatre e oche e contro la pratica dell'alimentazione forzata;

il tema è già da tempo all'attenzione della Commissione europea (Direzione generale dell'agricoltura e dello sviluppo rurale) che, nell'ambito della revisione delle norme sulla commercializzazione per la carne di pollame, ad aprile 2023 ha lanciato una consultazione pubblica. Il 90 per cento chiede l'eliminazione del requisito dei pesi minimi del fegato, per permettere ai consumatori di scegliere *foie gras* prodotto senza alimentazione forzata. Tra i *feedback* contro l'alimentazione forzata, spicca quello di *Coop Italia*, azienda

leader nel settore della grande distribuzione organizzata;

si rammenta inoltre che il 30 giugno 2023 al Parlamento europeo è stata presentata un'interrogazione a risposta scritta, firmata da ben 84 parlamentari europei, 15 di questi italiani e appartenenti ad ogni schieramento politico, con la quale si richiede l'eliminazione del requisito dei pesi minimi del fegato di anatre e oche e, quindi, di permettere la produzione di *foie gras* senza *gavage* –:

se non si intendano avviare in sede di Unione europea e nei confronti del Commissario europeo per l'agricoltura tutte le iniziative di competenza volte a ottenere la soppressione del requisito dei pesi minimi del fegato di anatre e oche, attualmente presente nel suddetto regolamento (CE) n. 543 del 2008. (3-01196)

DISEGNO DI LEGGE: DISPOSIZIONI IN MATERIA DI RAFFORZAMENTO DELLA CYBERSICUREZZA NAZIONALE E DI REATI INFORMATICI (A.C. 1717-A)

A.C. 1717-A – Parere della V Commissione

PARERE DELLA V COMMISSIONE SUL TESTO DEL PROVVEDIMENTO E SULLE PROPOSTE EMENDATIVE PRESENTATE

Sul testo del provvedimento in oggetto:

PARERE FAVOREVOLE

con le seguenti condizioni, volte a garantire il rispetto dell'articolo 81 della Costituzione:

All'articolo 8, sopprimere i commi da 7 a 11.

Conseguentemente, alla rubrica, sopprimere le parole: e rafforzamento della sicurezza delle modalità di accesso a banche di dati pubbliche.

All'articolo 10, comma 1, capoverso « mbis »*, terzo periodo, dopo le parole:* presso l'Agenzia *aggiungere le seguenti: ,* nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica.

Sugli emendamenti trasmessi dall'Assemblea:

PARERE CONTRARIO

sulle proposte emendative 1.101, 1.102, 1.103,2.6,2.7, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.10, 8.11, 8.15, 8.16, 8.20,10.023, 10.024,12.100,23.1, 23.3,23.4,23.5,23.12 e 23.13, in quanto suscettibili di determinare nuovi o maggiori oneri per la finanza pubblica privi di idonea quantificazione e copertura;

NULLA OSTA

sulle restanti proposte emendative.

A.C. 1717-A – Articolo 1

ARTICOLO 1 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI

CAPO I

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

Art. 1.

(Obblighi di notifica di incidenti)

1. Le pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, le regioni e le province autonome

di Trento e di Bolzano, le città metropolitane, i comuni con popolazione superiore a 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e le aziende sanitarie locali segnalano e notificano, con le modalità e nei termini di cui al comma 2, gli incidenti indicati nella tassonomia di cui all'articolo 1, comma 3-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, aventi impatto su reti, sistemi informativi e servizi informatici. Tra i soggetti di cui al presente comma sono altresì comprese le rispettive società *in house* che forniscono servizi informatici, i servizi di trasporto di cui al primo periodo del presente comma ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008.

2. I soggetti di cui al comma 1 segnalano, senza ritardo e comunque entro il termine massimo di ventiquattro ore dal momento in cui ne sono venuti a conoscenza a seguito delle evidenze comunque ottenute, qualunque incidente riconducibile a una delle tipologie individuate nella tassonomia di cui al comma 1 ed effettuano, entro settantadue ore a decorrere dal medesimo momento, la notifica completa di tutti gli elementi informativi disponibili. La segnalazione e la successiva notifica sono effettuate tramite le apposite procedure disponibili nel sito *internet* istituzionale dell'Agenzia per la cybersicurezza nazionale.

3. Per i comuni con popolazione superiore a 100.000 abitanti e i comuni capoluoghi di regione, per le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, per le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane, per le aziende sanitarie locali e per le società *in house* che forniscono servizi informatici, i servizi di trasporto di cui al presente comma ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008, gli obblighi di cui ai commi 1 e 2 del presente articolo si applicano a decorrere dal centottantesimo giorno successivo alla data di entrata in vigore della presente legge.

4. Nell'ipotesi in cui i soggetti di cui al comma 1 effettuino notifiche volontarie di incidenti al di fuori dei casi indicati nella tassonomia di cui al medesimo comma 1, si applicano le disposizioni di cui all'articolo 18, commi 3, 4 e 5, del decreto legislativo 18 maggio 2018, n. 65.

5. Nel caso di inosservanza dell'obbligo di notifica di cui ai commi 1 e 2, l'Agenzia per la cybersicurezza nazionale comunica all'interessato che la reiterazione dell'inosservanza, nell'arco di cinque anni, comporterà l'applicazione delle disposizioni di cui al comma 6 e può disporre, nei dodici mesi successivi all'accertamento del ritardo o dell'omissione, l'invio di ispezioni, anche al fine di verificare l'attuazione, da parte dei soggetti interessati dall'incidente, di interventi di rafforzamento della resilienza agli stessi, direttamente indicati dall'Agenzia per la cybersicurezza nazionale ovvero previsti da apposite linee guida adottate dalla medesima Agenzia. Le modalità di tali ispezioni sono disciplinate con determinazione del direttore generale dell'Agenzia per la cybersicurezza nazionale, pubblicata nella *Gazzetta Ufficiale*.

6. Nei casi di reiterata inosservanza, nell'arco di cinque anni, dell'obbligo di notifica di cui ai commi 1 e 2, l'Agenzia per la cybersicurezza nazionale applica altresì,

nel rispetto delle disposizioni dell'articolo 17, comma 4-*quater*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000 a carico dei soggetti di cui al comma 1. La violazione delle disposizioni del comma 1 del presente articolo può costituire causa di responsabilità disciplinare e amministrativo-contabile per i funzionari e i dirigenti responsabili.

7. Fermi restando gli obblighi e le sanzioni, anche penali, previsti da altre norme di legge, le disposizioni del presente articolo non si applicano:

a) ai soggetti di cui di cui all'articolo 3, comma 1, lettere *g)* e *i),* del decreto legislativo n. 65 del 2018 e a quelli di cui all'articolo 1, comma 2-*bis*, del decreto-legge n. 105 del 2019, convertito, con modificazioni, dalla legge n. 133 del 2019;

b) agli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124.

PROPOSTE EMENDATIVE

ART. 1.

(Obblighi di notifica di incidenti)

Al comma 1, secondo periodo, aggiungere, in fine, le seguenti parole: , qualora gestiscano dati o servizi che rientrino nel perimetro di sicurezza di cui al periodo precedente.

Conseguentemente, al medesimo articolo:

al comma 5, primo periodo, sostituire le parole: che la reiterazione dell'inosservanza, nell'arco di cinque anni, comporterà l'applicazione delle *con le seguenti*: , notificando la comunicazione all'Agenzia per l'Italia Digitale, che, a partire dalla terza inosservanza verranno applicate le;

al comma 6, primo periodo:

sostituire le parole: Nei casi di reiterata inosservanza *con le seguenti*: A partire dalla terza inosservanza;

dopo le parole: euro 125.000 *aggiungere le seguenti*: qualora l'inadempienza non sia stata già oggetto di provvedimento sanzionatorio ai sensi del comma 5 dell'articolo 18-*bis* del decreto legislativo 7 marzo 2005, n. 82.

1.100. Zaratti, Dori.

Al comma 1, aggiungere, in fine, il seguente periodo: L'Agenzia per la cybersicurezza nazionale, con proprio provvedimento, individua le società *in house* le quali, sulla base della loro attività e del loro ambito di servizio, sono ricomprese tra i soggetti di cui al presente comma.

1.15. Alfonso Colucci, Alifano, Auriemma, Penza, D'Orso, Ascari, Cafiero De Raho, Giuliano.

Dopo il comma 1, aggiungere il seguente:

1-*bis*. Per le finalità di cui alla presente legge, per l'anno 2024, per le pubbliche amministrazioni centrali di cui al comma 1 e l'Agenzia per la cybersicurezza nazionale di cui al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, sono stanziati 50 milioni di euro per l'acquisto di strumentazione tecnologiche atte al rafforzamento della cybersicurezza.

Conseguentemente, all'articolo 23:

al comma 1, primo periodo, premettere la parole: Fermo restando quanto previsto dal comma 1-*bis*,;

dopo il comma 1, aggiungere il seguente:

1-*bis*. Ai maggiori oneri derivanti dalla disposizione di cui al comma 1-*bis* dell'articolo 1, pari a 50 milioni di euro per l'anno 2024, si provvede mediante corrispondente

riduzione dell'autorizzazione di spesa di cui all'articolo 1, comma 272 della legge 30 dicembre 2023, n. 213.

1.101. Dori, Zaratti.

Dopo il comma 1, aggiungere il seguente:

1-*bis*. Per le finalità di cui alla presente legge, per l'anno 2024, per le pubbliche amministrazioni centrali di cui al comma 1 e l'Agenzia per la cybersicurezza nazionale di cui al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, sono stanziati 40 milioni di euro per l'acquisto di strumentazione tecnologiche atte al rafforzamento della cybersicurezza.

Conseguentemente, all'articolo 23:

al comma 1, primo periodo, premettere la parole: Fermo restando quanto previsto dal comma 1-*bis*,;

dopo il comma 1, aggiungere il seguente:

1-*bis*. Ai maggiori oneri derivanti dalla disposizione di cui al comma 1-*bis* dell'articolo 1, pari a 40 milioni di euro per l'anno 2024, si provvede mediante corrispondente riduzione dell'autorizzazione di spesa di cui all'articolo 1, comma 272 della legge 30 dicembre 2023, n. 213.

1.102. Dori, Zaratti.

Dopo il comma 1, aggiungere il seguente:

1-*bis*. Per le finalità di cui alla presente legge, per l'anno 2024, per le pubbliche amministrazioni centrali di cui al comma 1 e l'Agenzia per la cybersicurezza nazionale di cui al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, sono stanziati 30 milioni di euro per l'acquisto di strumentazione tecnologiche atte al rafforzamento della cybersicurezza.

Conseguentemente, all'articolo 23:

al comma 1, primo periodo, premettere la parole: Fermo restando quanto previsto dal comma 1-*bis*,;

dopo il comma 1, aggiungere il seguente:

1-*bis*. Ai maggiori oneri derivanti dalla disposizione di cui al comma 1-*bis* dell'articolo 1, pari a 30 milioni di euro per l'anno 2024 si provvede mediante corrispondente riduzione dell'autorizzazione di spesa di cui all'articolo 1, comma 272 della legge 30 dicembre 2023, n. 213.

1.103. Dori, Zaratti.

Al comma 5, primo periodo, dopo le parole: all'interessato *aggiungere le seguenti:* , notificando la comunicazione all'Agenzia per l'Italia digitale,.

1.20. Bonafè, Cuperlo, Fornaro, Mauri, Serracchiani, Di Biase, Zan, Lacarra, Gianassi, Casu.

Al comma 5, secondo periodo, aggiungere, in fine, le seguenti parole: unitamente alla definizione delle esigenze di natura tecnico-organizzativa che motivano l'eccezione alla comminazione delle sanzioni di cui all'articolo 2, comma 2.

1.22. Alifano, Alfonso Colucci, Auriemma, Penza, D'Orso, Ascari, Cafiero De Raho, Giuliano.

A.C. 1717-A – Articolo 2

ARTICOLO 2 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI

Art. 2.

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

1. I soggetti di cui all'articolo 1, comma 1, della presente legge e quelli di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21

settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, all'articolo 3, comma 1, lettere *g)* e *i)*, del decreto legislativo 18 maggio 2018, n. 65, e all'articolo 40, comma 3, alinea, del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259, in caso di segnalazioni puntuali dell'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità cui essi risultino potenzialmente esposti, provvedono, senza ritardo e comunque non oltre quindici giorni dalla comunicazione, all'adozione degli interventi risolutivi indicati dalla stessa Agenzia.

2. La mancata o ritardata adozione degli interventi risolutivi di cui al comma 1 comporta l'applicazione delle sanzioni di cui all'articolo 1, comma 6, salvo il caso in cui motivate esigenze di natura tecnico-organizzativa, tempestivamente comunicate all'Agenzia per la cybersicurezza nazionale, ne impediscano l'adozione o ne comportino il differimento oltre il termine indicato al comma 1.

PROPOSTE EMENDATIVE

ART. 2.

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

Al comma 1, sostituire le parole da: vulnerabilità *fino a:* comunicazione *con le seguenti:* e pubblicamente conosciute vulnerabilità cui essi risultino esposti, provvedono, senza ritardo e comunque non oltre trenta giorni dalla segnalazione.

Conseguentemente, al medesimo articolo, comma 2, dopo le parole: comma 1 *aggiungere le seguenti:* per oltre due volte nell'arco di un anno.

2.4. Mauri, Bonafè, Cuperlo, Fornaro, Gianassi, Serracchiani, Di Biase, Zan, Lacarra, Casu.

Al comma 1, aggiungere, in fine, le seguenti parole: a valere sulle risorse economiche all'occorrenza messe a disposizione dalla medesima Agenzia.

Conseguentemente:

al medesimo articolo, dopo il comma 1, aggiungere il seguente:

1-*bis*. Per l'attuazione del comma 1 il Ministero dell'interno assegna all'Agenzia uno stanziamento pari a 60 milioni di euro per ciascuno degli anni 2024 e 2025 che confluiscono nelle entrate dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 11, comma 2, lettera *f)*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.;

all'articolo 8:

al comma 1, alinea, sostituire le parole: nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente *con le seguenti:* nell'ambito delle risorse di cui al comma 2-*bis;*

dopo il comma 2, aggiungere i seguenti:

2-*bis*. A parziale o totale reintegro delle spese sostenute, nell'ambito delle risorse assegnate all'Agenzia nel limite massimo di 40 milioni di euro per ciascuno degli anni 2024 e 2025, la medesima Agenzia provvede annualmente al riparto in favore dei soggetti di cui all'articolo 1, che attivano le strutture di cui al comma 1 e individuano il referente di cui al comma 2, dietro presentazione della domanda redatta sulla base delle modalità e dei criteri indicati dalla medesima Agenzia.

2-*ter*. Le strutture di cui al comma 1 e il personale dei soggetti di cui all'articolo 1 sono tenuti a seguire periodicamente attività formative su tematiche di *cybersecurity* per sviluppare una cultura *cyber*, incrementare la consapevolezza e le competenze specialistiche e divulgare buone pratiche per la prevenzione e la gestione di potenziali attacchi. A parziale o totale reintegro delle spese sostenute per l'attuazione del presente comma, nell'ambito delle risorse

assegnate all'Agenzia nel limite massimo di 50 milioni di euro per ciascuno degli anni 2024 e 2025, la medesima Agenzia provvede annualmente al riparto in favore dei soggetti di cui all'articolo 1, dietro presentazione della domanda redatta sulla base delle modalità e dei criteri indicati dalla medesima Agenzia.;

all'articolo 23, sostituire il comma 1 con il seguente:

1. Per l'attuazione delle disposizioni di cui all'articolo 2, comma 1-*bis* e all'articolo 8, commi 2-*bis* e 2-*ter*, il Ministero dell'interno assegna all'Agenzia uno stanziamento pari a 150 milioni di euro per ciascuno degli anni 2024 e 2025 che confluiscono nelle entrate dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 11, comma 2, lettera *f)*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109. Agli oneri derivanti dall'attuazione delle disposizioni di cui al presente comma pari a 150 milioni di euro per ciascuno degli anni 2024 e 2025, si provvede mediante corrispondente riduzione del Fondo per interventi strutturali di politica economica di cui all'articolo 10, comma 5, del decreto-legge 29 novembre 2004, n. 282, convertito, con modificazioni, dalla legge 27 dicembre 2004, n. 307.

2.6. Bonafè, Mauri, Cuperlo, Fornaro, Serracchiani, Di Biase, Zan, Lacarra, Gianassi, Casu.

Al comma 1, aggiungere, in fine, le seguenti parole: a valere sulle risorse economiche all'occorrenza messe a disposizione dalla medesima Agenzia.

Conseguentemente:

al medesimo articolo, dopo il comma 1, aggiungere il seguente:

1-*bis*. Per l'attuazione del comma 1 il Ministero dell'interno assegna all'Agenzia uno stanziamento pari a 60 milioni di euro per ciascuno degli anni 2024 e 2025 che confluiscono nelle entrate dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 11, comma 2, lettera *f)*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

all'articolo 23, sostituire il comma 1 con il seguente:

1. Agli oneri derivanti dall'attuazione delle disposizioni di cui all'articolo 2, comma 1-*bis*, della presente legge, pari a 60 milioni di euro per ciascuno degli anni 2024 e 2025, si provvede mediante corrispondente riduzione del Fondo per interventi strutturali di politica economica di cui all'articolo 10, comma 5, del decreto-legge 29 novembre 2004, n. 282, convertito, con modificazioni, dalla legge 27 dicembre 2004, n. 307.

2.7. Bonafè, Mauri, Cuperlo, Fornaro, Serracchiani, Di Biase, Zan, Lacarra, Gianassi, Casu.

A.C. 1717-A – Articolo 3

ARTICOLO 3 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI IDENTICO A QUELLO DEL GOVERNO

Art. 3.

(Norme di raccordo con le disposizioni del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133)

1. All'articolo 1, comma 3-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, sono apportate le seguenti modificazioni:

a) il secondo periodo è sostituito dal seguente: « I medesimi soggetti provvedono a effettuare la segnalazione degli incidenti di cui al presente comma senza ritardo, comunque entro il termine massimo di ventiquattro ore, e ad effettuare la relativa notifica entro settantadue ore »;

b) dopo il quarto periodo è inserito il seguente: « Nei casi di reiterata inosservanza degli obblighi di notifica di cui al presente comma, si applica la sanzione

amministrativa pecuniaria da euro 25.000 a euro 125.000 ».

PROPOSTA EMENDATIVA

ART. 3.

(Norme di raccordo con le disposizioni del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133)

Sopprimerlo.

3.1. Mauri, Bonafè, Cuperlo, Fornaro, Gianassi, Serracchiani, Di Biase, Zan, Lacarra, Casu.

A.C. 1717-A – Articolo 4

ARTICOLO 4 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI

Art. 4.

(Disposizioni in materia di dati relativi a incidenti informatici)

1. All'articolo 7, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, dopo la lettera *n-bis)* è inserita la seguente:

« *n-ter)* provvede alla raccolta, all'elaborazione e alla classificazione dei dati relativi alle notifiche di incidenti ricevute dai soggetti che a ciò siano tenuti in osservanza delle disposizioni vigenti. Tali dati sono resi pubblici nell'ambito della relazione prevista dall'articolo 14, comma 1, quali dati ufficiali di riferimento degli attacchi informatici portati ai soggetti che operano nei settori rilevanti per gli interessi nazionali nel campo della cybersicurezza. A tali adempimenti si provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente ».

A.C. 1717-A – Articolo 5

ARTICOLO 5 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI IDENTICO A QUELLO DEL GOVERNO

Art. 5.

(Disposizioni in materia di Nucleo per la cybersicurezza)

1. All'articolo 8 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, dopo il comma 4 è inserito il seguente:

« *4.1*. In relazione a specifiche questioni di particolare rilevanza concernenti i compiti di cui all'articolo 9, comma 1, lettera *a)*, il Nucleo può essere convocato nella composizione di cui al comma 4, di volta in volta estesa alla partecipazione di un rappresentante della Direzione nazionale antimafia e antiterrorismo, della Banca d'Italia o di uno o più operatori di cui all'articolo 1, comma 2-*bis*, del decreto-legge perimetro, nonché di eventuali altri soggetti, interessati alle stesse questioni. Le amministrazioni e i soggetti convocati partecipano alle suddette riunioni a livello di vertice ».

A.C. 1717-A – Articolo 6

ARTICOLO 6 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI IDENTICO A QUELLO DEL GOVERNO

Art. 6.

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

1. Qualora i servizi di cui agli articoli 6 e 7 della legge 3 agosto 2007, n. 124, avuta notizia di un evento o un incidente informatici, ritengano strettamente necessario, per il perseguimento delle finalità istituzio-

nali del Sistema di informazione per la sicurezza della Repubblica, il differimento di una o più delle attività di resilienza di cui all'articolo 7, comma 1, lettere *n)* e *n-bis)*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, i predetti servizi, per il tramite del Dipartimento delle informazioni per la sicurezza, ne informano il Presidente del Consiglio dei ministri o l'Autorità delegata di cui all'articolo 3 della citata legge n. 124 del 2007, ove istituita.

2. Nei casi di cui al comma 1, il Presidente del Consiglio dei ministri, sentiti il direttore generale del Dipartimento delle informazioni per la sicurezza e il direttore generale dell'Agenzia per la cybersicurezza nazionale, può disporre il differimento degli obblighi informativi cui è in ogni caso tenuta l'Agenzia ai sensi delle disposizioni vigenti, ivi compresi quelli previsti ai sensi dell'articolo 17, commi 4 e 4-*bis*, del decreto-legge n. 82 del 2021, nonché il differimento di una o più delle attività di resilienza di cui all'articolo 7, comma 1, lettere *n)* e *n-bis)*, del medesimo decreto-legge.

A.C. 1717-A – Articolo 7

ARTICOLO 7 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI

Art. 7.

(Composizione del Comitato interministeriale per la sicurezza della Repubblica)

1. All'articolo 5, comma 3, della legge 3 agosto 2007, n. 124, sono apportate le seguenti modificazioni:

a) dopo le parole: « Ministro degli affari esteri » sono inserite le seguenti: « e della cooperazione internazionale »;

b) le parole: « dello sviluppo economico e dal Ministro della transizione ecologica » sono sostituite dalle seguenti: « delle imprese e del *made in Italy*, dal Ministro dell'ambiente e della sicurezza energetica, dal Ministro dell'agricoltura, della sovranità alimentare e delle foreste, dal Ministro delle infrastrutture e dei trasporti e dal Ministro dell'università e della ricerca ».

A.C. 1717-A – Articolo 8

ARTICOLO 8 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI

Art. 8.

(Rafforzamento della resilienza delle pubbliche amministrazioni, referente per la cybersicurezza e rafforzamento della sicurezza delle modalità di accesso a banche di dati pubbliche)

1. I soggetti di cui all'articolo 1, comma 1, individuano, ove non sia già presente, una struttura, anche tra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, che provvede:

a) allo sviluppo delle politiche e procedure di sicurezza delle informazioni;

b) alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico;

c) alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione;

d) alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione;

e) alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere *b)* e *d)*;

f) alla pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale;

g) al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.

2. Presso le strutture di cui al comma 1 opera il referente per la cybersicurezza, individuato in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza. Nel caso in cui i soggetti di cui all'articolo 1, comma 1, non dispongano di personale dipendente fornito di tali requisiti, possono conferire l'incarico di referente per la cybersicurezza a un dipendente di una pubblica amministrazione, previa autorizzazione di quest'ultima ai sensi dell'articolo 53 del decreto legislativo 30 marzo 2001, n. 165, nell'ambito delle risorse disponibili a legislazione vigente. Il referente per la cybersicurezza svolge anche la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale in relazione a quanto previsto dalla presente legge e dalle normative settoriali in materia di cybersicurezza cui è soggetta la medesima amministrazione. A tal fine, il nominativo del referente per la cybersicurezza è comunicato all'Agenzia per la cybersicurezza nazionale.

3. La struttura e il referente di cui ai commi 1 e 2 possono essere individuati, rispettivamente, nell'ufficio e nel responsabile per la transizione al digitale previsti dall'articolo 17 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82.

4. I compiti di cui ai commi 1 e 2 possono essere esercitati in forma associata secondo quanto previsto dall'articolo 17, commi 1-*sexies* e 1-*septies*, del codice di cui al decreto legislativo 7 marzo 2005, n. 82.

5. L'Agenzia per la cybersicurezza nazionale può individuare modalità e processi di coordinamento e di collaborazione tra le amministrazioni di cui all'articolo 1, comma 1, e tra i referenti per la cybersicurezza di cui al comma 2 del presente articolo, al fine di facilitare la resilienza delle amministrazioni pubbliche.

6. Le disposizioni di cui al presente articolo non si applicano:

a) ai soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, ai quali continuano ad applicarsi gli obblighi previsti dalle disposizioni di cui alla richiamata disciplina;

b) agli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124.

7. Al fine di garantire adeguata tutela e protezione dai rischi di accesso abusivo ai dati contenuti in sistemi informatici delle pubbliche amministrazioni, per l'accesso alle banche di dati pubbliche da parte di addetti tecnici e di soggetti incaricati del trattamento dei dati in esse contenuti è richiesto l'utilizzo di specifici sistemi di autenticazione informatica, consistenti nell'uso combinato di almeno due differenti tecnologie di autenticazione, una delle quali sia basata sull'elaborazione di caratteristiche biometriche.

8. Ai fini del comma 7, si intendono per « addetti tecnici » gli operatori tecnici aventi funzioni di amministratori di sistema, di rete o di archivio di dati.

9. Limitatamente ai casi di interventi indifferibili relativi a malfunzionamenti, guasti, installazione di *hardware* e *software*, aggiornamento e riconfigurazione dei sistemi, che determinino la necessità di accesso ai sistemi informatici di cui al comma 7, l'accesso alle banche di dati pubbliche da parte dei soggetti di cui al comma 8 è consentito anche senza l'utilizzo di almeno due differenti tecnologie di autenticazione, di cui una basata sull'elaborazione di caratteristiche biometriche, in deroga alle disposizioni del comma 7, per le operazioni che richiedono la presenza fisica dell'addetto che procede all'intervento in prossimità del sistema di elaborazione.

10. Fatti salvi gli obblighi in materia di credenziali di cui al decreto legislativo 18 maggio 2018, n. 51, gli accessi di cui al comma 9 sono annotati in un apposito registro unitamente alle motivazioni che li hanno determinati e alla descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di apparecchiature elettroniche. Il registro degli accessi di cui al primo periodo è detenuto dal soggetto o dall'ente titolare della banca di dati, che lo aggiorna periodicamente, lo custodisce presso le sedi di elaborazione e lo mette a disposizione delle autorità, su richiesta, nel caso di ispezioni o controlli, unitamente all'elenco nominativo dei soggetti abilitati all'accesso ai sistemi di elaborazione titolari delle funzioni di cui al comma 8.

11. Le pubbliche amministrazioni adottano le misure di cui ai commi 7 e 10 entro dodici mesi dalla data di entrata in vigore della presente legge. All'attuazione delle disposizioni del presente articolo si provvede con le risorse umane, finanziarie e strumentali disponibili a legislazione vigente.

PROPOSTE EMENDATIVE

ART. 8.

(Rafforzamento della resilienza delle pubbliche amministrazioni, referente per la cybersicurezza e rafforzamento della sicurezza delle modalità di accesso a banche di dati pubbliche)

Al comma 1, alinea, sostituire le parole da: individuano *fino a:* a legislazione vigente *con le seguenti*: affidano a un unico ufficio, anche tra quelli eventualmente già esistenti, ai sensi dell'articolo 17, comma 1, primo periodo, e 1-*sexies*, del decreto legislativo 7 marzo 2005, n. 82.

8.1. Auriemma, Alfonso Colucci, Alifano, Penza, D'Orso, Ascari, Cafiero De Raho, Giuliano.

Al comma 1, alinea, sopprimere le parole: nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente,.

Conseguentemente:

al medesimo articolo,

dopo il comma 5, aggiungere i seguenti:

5-*bis*. Al fine di consentire, nell'ambito delle strutture di cui al comma 1, di disporre delle risorse umane, strumentali e finanziarie necessarie per l'attuazione delle disposizioni previste, è istituito, nello stato di previsione del Ministero dell'economia e delle finanze, un apposito capitolo con una dotazione di 200 milioni di euro per ciascuno degli anni 2024, 2025 e 2026. Con decreto del Ministro dell'economia e delle finanze, adottato entro il mese di giugno di ciascuno degli anni 2024, 2025 e 2026, sono individuati i criteri del riparto delle risorse di cui al periodo precedente e i relativi destinatari.

5-*ter*. Agli oneri di cui al comma 5-*bis*, pari a 200 milioni di euro per ciascuno degli anni 2024, 2025 e 2026, si provvede mediante corrispondente riduzione del Fondo di cui all'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190.

5-*quater*. Ai fini dell'attuazione delle disposizioni di cui ai commi precedenti, il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.;

al comma 11, secondo periodo, premettere le parole: Fermo restando quanto previsto dai commi 5-*bis*, 5-*ter* e 5-*quater*, ;

all'articolo 23, sopprimere il comma 1.

8.3. Boschi.

Al comma 1, alinea, sopprimere le parole: nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente,.

Conseguentemente:

al medesimo articolo,

dopo il comma 5, aggiungere i seguenti:

5-*bis*. Al fine di consentire, nell'ambito delle strutture di cui al comma 1, di di-

sporre delle dotazioni tecnologiche necessarie per l'attuazione delle disposizioni previste, è istituito, nello stato di previsione del Ministero dell'economia e delle finanze, un apposito capitolo con una dotazione di 200 milioni di euro per ciascuno degli anni 2024, 2025 e 2026. Con decreto del Ministro dell'economia e delle finanze, adottato entro il mese di giugno di ciascuno degli anni 2024, 2025 e 2026, sono individuati i criteri del riparto delle risorse di cui al periodo precedente e i relativi destinatari.

5-*ter*. Agli oneri di cui al comma 5-*bis*, pari a 200 milioni di euro per ciascuno degli anni 2024, 2025 e 2026, si provvede mediante corrispondente riduzione del Fondo di cui all'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190.

5-*quater*. Ai fini dell'attuazione delle disposizioni di cui ai commi precedenti, il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.;

al comma 11, secondo periodo, premettere le parole: Fermo restando quanto previsto dai commi 5-*bis*, 5-*ter* e 5-*quater*, ;

all'articolo 23, sopprimere il comma 1.

8.2. Boschi.

Al comma 1, alinea, sopprimere le parole: nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente,.

Conseguentemente,

al medesimo articolo, comma 11, secondo periodo, dopo le parole: delle disposizioni *aggiungere le seguenti*: dei commi da 6 a 10*;*

all'articolo 23:

al comma 1, primo periodo, premettere le parole: Fermo restando quanto previsto dai commi 2, 2-*bis* e 2-*ter* del presente articolo, ;

sostituire il comma 2 con i seguenti:

2. Al fine di consentire, ai soggetti di cui all'articolo 1, comma 1, di disporre delle risorse umane, strumentali e finanziarie necessarie per l'attuazione delle disposizioni di cui all'articolo 8, comma 1, è istituito, nello stato di previsione del Ministero dell'economia e delle finanze, un apposito fondo, con una dotazione di 200 milioni di euro per ciascuno degli anni 2024, 2025 e 2026.

2-*bis*. Con decreto del Ministro dell'economia e delle finanze, adottato entro il mese di giugno di ciascuno degli anni 2024, 2025 e 2026, sono individuati i criteri del riparto delle risorse di cui al comma precedente e i relativi destinatari.

2-*ter*. Agli oneri di cui al comma 2, pari a 200 milioni di euro per ciascuno degli anni 2024, 2025 e 2026, si provvede mediante corrispondente riduzione del Fondo di cui all'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190.

8.4. Boschi.

Al comma 1, alinea, sostituire le parole: umane, strumentali e finanziarie disponibili a legislazione vigente, *con le seguenti*: di cui al comma 2-*bis*.

Conseguentemente:

al medesimo articolo, dopo il comma 2, aggiungere i seguenti:

2-*bis*. A parziale o totale reintegro delle spese sostenute, nell'ambito delle risorse assegnate all'Agenzia nel limite massimo di 40 milioni di euro per ciascuno degli anni 2024 e 2025, la medesima Agenzia provvede annualmente al riparto in favore dei soggetti di cui all'articolo 1, che attivano le strutture di cui al comma 1 e individuano il referente di cui al comma 2, dietro presentazione della domanda redatta sulla base delle modalità e dei criteri indicati dalla medesima Agenzia.

2-*ter*. Per l'attuazione del comma 2-*bis* il Ministero dell'interno assegna all'Agenzia uno stanziamento pari a 40 milioni di euro per ciascuno degli anni 2024 e 2025 che confluiscono nelle entrate dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 11, comma 2, lettera *f)*, del decreto-legge 14 giugno 2021, n. 82, convertito, con

modificazioni, dalla legge 4 agosto 2021, n. 109.

all'articolo 23, sostituire il comma 1 con il seguente:

1. Agli oneri derivanti dall'attuazione delle disposizioni di cui all'articolo 8, comma 2-*ter*, della presente legge, pari a 40 milioni di euro per ciascuno degli anni 2024 e 2025, si provvede mediante corrispondente riduzione del Fondo per interventi strutturali di politica economica di cui all'articolo 10, comma 5, del decreto-legge 29 novembre 2004, n. 282, convertito, con modificazioni, dalla legge 27 dicembre 2004, n. 307.

8.5. Bonafè, Mauri, Cuperlo, Fornaro, Serracchiani, Di Biase, Zan, Lacarra, Gianassi, Casu.

Al comma 1, alinea, sostituire le parole: umane, strumentali e finanziarie disponibili a legislazione vigente *con le seguenti:* finanziarie messe a disposizione dalla presente legge.

8.6. Mauri, Bonafè, Cuperlo, Fornaro, Gianassi, Serracchiani, Di Biase, Zan, Lacarra, Casu.

Al comma 2, sostituire il primo periodo con i seguenti:

2. Presso gli uffici di cui al comma 1 opera il referente per la cybersicurezza, in possesso delle competenze di cui all'articolo 17, comma 1-*ter*, del decreto legislativo 7 marzo 2005, n. 82, nonché in materia di strategie e tecnologie di sicurezza informatica e cibernetica. Le Linee guida di cui all'articolo 1, comma 1, definiscono le modalità di aggiornamento professionale del referente, al fine di rafforzare la capacità di resilienza e risposta delle pubbliche amministrazioni alle minacce e ai rischi informatici e alla loro continua evoluzione, in linea con gli obiettivi della direttiva 2022/255. Il referente opera d'intesa e in collaborazione con il Responsabile per la transizione digitale di cui all'articolo 17, del predetto decreto legislativo e con il Responsabile della protezione dei dati (RDP), di cui all'articolo 37 del Regolamento generale sulla protezione dei dati personali n. 2016/679.

8.8. Alfonso Colucci, Alifano, Auriemma, Penza, D'Orso, Ascari, Cafiero De Raho, Giuliano.

Al comma 2, primo periodo, dopo le parole: Presso le strutture di cui al comma 1 *aggiungere le seguenti*: , d'intesa e in collaborazione con il Responsabile per la transizione digitale di cui all'articolo 17 del decreto legislativo 7 marzo 2005, n. 82 e il Responsabile della protezione dei dati (RPD) di cui all'articolo 37 del regolamento europeo 2016/679,.

8.9. Boschi.

Al comma 2, primo periodo, sostituire le parole da: il referente per la cybersicurezza*, fino alla fine del periodo con le seguenti:* , in coordinamento con il Responsabile per la Transizione Digitale (RTD), il referente per la cybersicurezza, individuato, anche al di fuori della pianta organica dei soggetti di cui all'articolo 1, entro un periodo di dodici mesi dalla data di entrata in vigore della presente legge, in ragione delle qualità professionali possedute. Il nominativo del referente per la cybersicurezza è comunicato all'Agenzia per la cybersicurezza nazionale entro le ventiquattro ore successive alla nomina. L'Agenzia per la cybersicurezza nazionale individua, entro tre mesi dalla data di entrata in vigore della presente legge, le competenze specifiche minime necessarie a ricoprire il ruolo di referente per la cybersicurezza di cui al presente comma. L'Agenzia si impegna, inoltre, ad offrire strumenti di formazione atti a garantire un'adeguata preparazione al referente per la cybersicurezza. Il referente per la cybersicurezza svolge, altresì, la funzione di raccordo tra l'amministrazione di appartenenza e l'Agenzia per la cybersicurezza nazionale in relazione a quanto previsto dalla presente legge e dalle normative di settore in materia di cybersi-

curezza cui è soggetta la medesima amministrazione.

8.10. Pastorella.

Al comma 2 , sostituire le parole da: in ragione di *fino a:* . Il referente per la cybersicurezza *con le seguenti:* tra i dipendenti dell'Amministrazione, aventi il requisito di essere tecnici abilitati iscritti all'albo di cui all'articolo 45, comma 1, lettera *c)*, del decreto Presidente della Repubblica 5 giugno 2001, n. 328. Nel caso in cui all'interno della Pubblica Amministrazione non vi fossero dipendenti con tali requisiti l'ente potrà incaricare un dipendente di altra Pubblica Amministrazione o professionisti esterni in possesso dei requisiti. Il predetto referente.

8.11. Manzi, Mauri.

Dopo il comma 2, aggiungere i seguenti:

2-*bis*. L'Agenzia per la cybersicurezza nazionale, organizza, periodicamente, e comunque ogni dodici mesi, anche in partenariato con soggetti pubblici e privati, corsi di formazione specifici per il ruolo di referente per la cybersicurezza di cui al comma precedente, cui devono partecipare i referenti per la cybersicurezza operanti presso i soggetti di cui all'articolo 1, comma 1.

2-*ter*. Per le finalità di cui al comma 2-*bis* è autorizzata la spesa di 100 milioni di euro per ciascuno degli anni 2024 e 2025, che incrementano la dotazione del capitolo di bilancio istituito presso il Ministero dell'economia e delle finanze, di cui all'articolo 18, comma 1 del decreto-legge 14 giugno 2021, n. 82, convertito con legge 4 agosto 2021, n. 109.

2-*quater*. Ai fini dell'attuazione delle disposizioni di cui al comma 2-*ter*, all'articolo 23, comma 1 del decreto-legge 14 giugno 2021, n. 82, convertito con legge 4 agosto 2021, n. 109, dopo le parole: « Per l'attuazione degli articoli da 5 a 7 », sono inserite le seguenti: « e al fine di predisporre corsi di formazione per i referenti per la cybersicurezza operanti presso le pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, le regioni e le province autonome di Trento e di Bolzano, le città metropolitane, i comuni con popolazione superiore a 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e le aziende sanitarie locali ».

Conseguentemente,

al medesimo articolo, comma 11, secondo periodo, premettere le parole: Fermo restando quanto previsto dai commi 2-*bis*, 2-*ter* e 2-*quater*, ;

all'articolo 23 sopprimere il comma 1.

8.15. Boschi.

Dopo il comma 2 aggiungere i seguenti:

2-*bis*. Le strutture di cui al comma 1 e il personale dei soggetti di cui all'articolo 1 sono tenuti a seguire periodicamente attività formative su tematiche di *cybersecurity* per sviluppare una cultura *cyber*, incrementare la consapevolezza e le competenze specialistiche e divulgare buone pratiche per la prevenzione e la gestione di potenziali attacchi.

2-*ter* A parziale o totale reintegro delle spese sostenute per l'attuazione dei corsi di cui al comma 2-*bis*, nell'ambito delle risorse assegnate all'Agenzia nel limite massimo di 50 milioni di euro per ciascuno degli anni 2024 e 2025, la medesima Agenzia provvede annualmente al riparto in favore dei soggetti di cui all'articolo 1, dietro presentazione della domanda redatta sulla base delle modalità e dei criteri indicati dalla medesima Agenzia.

2-*quater*. Per l'attuazione del comma 2-*ter* il Ministero dell'interno assegna all'Agenzia uno stanziamento pari a 50 milioni di euro per ciascuno degli anni 2024 e 2025 che confluiscono nelle entrate dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 11, comma 2, lettera *f)*, del decreto-legge 14 giugno 2021, n. 82,

convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

Conseguentemente,

al medesimo articolo, comma 11, secondo periodo, premettere le parole: Fermo restando quanto previsto dai commi 2-*bis*, 2-*ter* e 2-*quater*, ;

all'articolo 23, sostituire il comma 1 con il seguente:

1. Agli oneri derivanti dall'attuazione delle disposizioni di cui all'articolo 8, comma 2-*quater*, pari a 50 milioni di euro per ciascuno degli anni 2024 e 2025, si provvede mediante corrispondente riduzione del Fondo per interventi strutturali di politica economica di cui all'articolo 10, comma 5, del decreto-legge 29 novembre 2004, n. 282, convertito, con modificazioni, dalla legge 27 dicembre 2004, n. 307.

8.16. Bonafè, Mauri, Cuperlo, Fornaro, Serracchiani, Di Biase, Zan, Lacarra, Gianassi, Casu.

Dopo il comma 2, aggiungere il seguente:

2-*bis*. I soggetti di cui all'articolo 1, comma 1, prevedono lo sviluppo di adeguate competenze tecnologiche, di informatica giuridica e manageriali per la figura del Referente per la cybersicurezza e per coloro che operano nelle strutture da individuare ai sensi del presente articolo, anche attraverso partenariati tra soggetti pubblici e privati, in particolare con le Università, che possono vantare competenze e linee strategiche in materia, anche al fine di creare la consapevolezza, che costituisce parte integrante e indispensabile della cultura digitale.

8.20. Boschi.

Dopo il comma 2, aggiungere il seguente:

2-*bis*. Il personale impegnato nelle strutture per la cybersicurezza di cui al comma 1, è valutato ai fini del processo di misurazione e valutazione della performance anche in base al rispetto e all'attuazione delle disposizioni di cui ai commi 1 e 2 del presente articolo e al corretto adempimento degli obblighi ivi previsti, a fini di effettività ed efficacia.

8.21. Boschi.

Sopprimere i commi da 7 a 11.

Conseguentemente, alla rubrica, sopprimere le parole: e rafforzamento della sicurezza delle modalità di accesso a banche di dati pubbliche.

8.300. ***(da votare ai sensi dell'articolo 86, comma 4-bis, del Regolamento)***

(Approvato)

A.C. 1717-A – Articolo 9

ARTICOLO 9 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI

Art. 9.

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

1. Le strutture di cui all'articolo 8 nonché quelle che svolgono analoghe funzioni per i soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e al decreto legislativo 18 maggio 2018, n. 65, verificano che i programmi e le applicazioni informatiche e di comunicazione elettronica in uso, che utilizzano soluzioni crittografiche, rispettino le linee guida sulla crittografia nonché quelle sulla conservazione delle *password* adottate dall'Agenzia per la cybersicurezza nazionale e dal Garante per la protezione dei dati personali e che non comportino vulnerabilità note, atte a rendere disponibili e intellegibili a terzi i dati cifrati.

A.C. 1717-A – Articolo 10

ARTICOLO 10 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI

Art. 10.

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

1. All'articolo 7, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito,

con modificazioni, dalla legge 4 agosto 2021, n. 109, la lettera *m-bis)* è sostituita dalla seguente:

« *m-bis)* provvede, anche attraverso un'apposita sezione nell'ambito della strategia di cui alla lettera *b)*, allo sviluppo e alla diffusione di *standard*, linee guida e raccomandazioni al fine di rafforzare la cybersicurezza dei sistemi informatici, alla valutazione della sicurezza dei sistemi crittografici nonché all'organizzazione e alla gestione di attività di divulgazione finalizzate a promuovere l'utilizzo della crittografia come strumento di cybersicurezza. L'Agenzia, anche per il rafforzamento dell'autonomia industriale e tecnologica dell'Italia, promuove altresì la collaborazione con centri universitari e di ricerca per la valorizzazione dello sviluppo di nuovi algoritmi proprietari, la ricerca e il conseguimento di nuove capacità crittografiche nazionali nonché la collaborazione internazionale con gli organismi esteri che svolgono analoghe funzioni. A tale fine, è istituito presso l'Agenzia il Centro nazionale di crittografia, il cui funzionamento è disciplinato con provvedimento del direttore generale dell'Agenzia stessa. Il Centro nazionale di crittografia svolge le funzioni di centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato, ferme restando le competenze dell'Ufficio centrale per la segretezza, di cui all'articolo 9 della legge 3 agosto 2007, n. 124, con riferimento alle informazioni e alle attività previste dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della citata legge n. 124 del 2007, nonché le competenze degli organismi di cui agli articoli 4, 6 e 7 della medesima legge ».

PROPOSTE EMENDATIVE

ART. 10.

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

Al comma 1, capoverso m-bis), *dopo le parole:* l'utilizzo della crittografia *aggiungere le seguenti:* , anche attraverso la tecnologia *blockchain*,.

10.15. Boschi.

Al comma 1, capoverso m-bis), *dopo le parole:* l'utilizzo della crittografia *aggiungere le seguenti:* , anche a vantaggio della tecnologia *blockchain*,.

10.15. *(Testo modificato nel corso della seduta)* Boschi.

(Approvato)

Al comma 1, capoverso « m-bis », *terzo periodo, dopo le parole:* presso l'Agenzia *aggiungere le seguenti:* , nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica.

10.300. ***(da votare ai sensi dell'articolo 86, comma 4-bis, del Regolamento)***

(Approvato)

Dopo l'articolo 10, aggiungere il seguente:

Art. 10-*bis*.

(Iniziative per la diffusione della cultura della sicurezza informatica)

1. L'Agenzia per la cybersicurezza nazionale, d'intesa con l'Agenzia per l'Italia digitale e i soggetti di cui all'articolo 1, comma 1, coordina la realizzazione e la promozione, anche con il coinvolgimento di Università, Centri di ricerca e di formazione specializzati, di iniziative volte a favorire la diffusione della cultura della sicurezza informatica tra i cittadini, con particolare riguardo alle categorie a rischio di esclusione, con azioni specifiche e concrete, anche avvalendosi di un insieme di strumenti e mezzi diversi, fra i quali il servizio radiotelevisivo. A tal fine è autorizzata la spesa di 10 milioni di euro per l'anno 2024.

2. Alla copertura degli oneri derivanti dall'attuazione del comma 1, pari a 10

milioni di euro per l'anno 2024, si provvede mediante corrispondente riduzione del Fondo di cui all'articolo 1, comma 199, della legge 23 dicembre 2014, n. 190.

Conseguentemente, all'articolo 23, sopprimere il comma 1.

10.023. Penza, Alfonso Colucci, Alifano, Auriemma, D'Orso, Ascari, Cafiero De Raho, Giuliano.

Dopo l'articolo 10, aggiungere il seguente:

Art. 10-*bis*.

(Iniziative in materia di sicurezza informatica nell'ambito del sistema educativo)

1. L'Agenzia per la cybersicurezza nazionale, d'intesa con il Ministro dell'istruzione e del merito, promuove la realizzazione di corsi specifici al fine di favorire in tutti i livelli del sistema educativo una progressiva familiarizzazione degli studenti con la sicurezza informatica. A tal fine, è autorizzata la spesa di 50 milioni di euro per i corsi da svolgersi nell'anno scolastico 2024-2025.

2. Alla copertura degli oneri derivanti dall'attuazione del comma 1, pari a 50 milioni di euro per l'anno 2024, si provvede mediante corrispondente riduzione del Fondo di cui all'articolo 1, comma 199, della legge 23 dicembre 2014, n. 190.

Conseguentemente, all'articolo 23, sopprimere il comma 1.

10.024. Penza, Alfonso Colucci, Alifano, Auriemma, D'Orso, Ascari, Cafiero De Raho, Giuliano.

A.C. 1717-A – Articolo 11

ARTICOLO 11 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI

Art. 11.

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

1. All'articolo 17 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, dopo il comma 4-*ter* è inserito il seguente:

« *4-quater*. La disciplina del procedimento sanzionatorio amministrativo dell'Agenzia è definita con regolamento che stabilisce, in particolare, termini e modalità per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia ai sensi del presente decreto e delle altre disposizioni che assegnano poteri accertativi e sanzionatori all'Agenzia. Il regolamento di cui al primo periodo è adottato, entro novanta giorni dalla data di entrata in vigore della presente disposizione, con decreto del Presidente del Consiglio dei ministri, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, sentito il Comitato interministeriale per la cybersicurezza e acquisito il parere delle competenti Commissioni parlamentari. Fino alla data di entrata in vigore del regolamento di cui al presente comma, ai procedimenti sanzionatori si applicano, per ciascuna fase procedimentale di cui al primo periodo, le disposizioni contenute nelle sezioni I e II del capo I della legge 24 novembre 1981, n. 689 ».

PROPOSTA EMENDATIVA

ART. 11.

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

Sopprimerlo

11.1. Boschi.

A.C. 1717-A – Articolo 12

ARTICOLO 12 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI

Art. 12.

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

1. All'articolo 12 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, dopo il comma 8-*bis* sono aggiunti i seguenti:

« *8-ter*. I dipendenti appartenenti al ruolo del personale dell'Agenzia di cui al comma 2, lettera *a)*, che abbiano partecipato, nell'interesse e a spese dell'Agenzia, a specifici percorsi formativi di specializzazione, per la durata di due anni a decorrere dalla data di completamento dell'ultimo dei predetti percorsi formativi non possono essere assunti né assumere incarichi presso soggetti privati al fine di svolgere mansioni in materia di cybersicurezza. I contratti stipulati in violazione di quanto disposto dal presente comma sono nulli. Le disposizioni del presente comma non si applicano al personale cessato dal servizio presso l'Agenzia secondo quanto previsto dalle disposizioni del regolamento adottato ai sensi del presente articolo relative al collocamento a riposo d'ufficio, al raggiungimento del requisito anagrafico previsto dalla legge per la pensione di vecchiaia, alla cessazione a domanda per inabilità o alla dispensa dal servizio per motivi di salute. I percorsi formativi di specializzazione di cui al presente comma sono individuati con determinazione del direttore generale dell'Agenzia, tenendo conto della particolare qualità dell'offerta formativa, dei costi, della durata e del livello di specializzazione che consegue alla frequenza dei suddetti percorsi.

8-quater. Il personale di cui ai commi 8 e 8.1 dell'articolo 17, entrato nel ruolo di cui al comma 2, lettera *a)*, del presente articolo, proveniente dalle Forze armate o dalle Forze di polizia ad ordinamento militare o civile di cui all'articolo 16 della legge 1° aprile 1981, n. 121, può rientrare, per motivate esigenze operative, nel ruolo dell'amministrazione di originaria provenienza, su richiesta della stessa, con l'assenso dell'interessato e del direttore generale dell'Agenzia. All'attuazione delle disposizioni del primo periodo, in relazione alla progressione di carriera, all'avanzamento e allo stato giuridico del personale proveniente dalle citate amministrazioni, si provvede con regolamento da adottare 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, sentito il Comitato interministeriale per la cybersicurezza, previo parere delle Commissioni parlamentari competenti per materia e per i profili finanziari e, per i profili di competenza, del Comitato parlamentare per la sicurezza della Repubblica, entro centoventi giorni dalla data di entrata in vigore della presente disposizione. Le disposizioni di cui al presente comma si applicano, nel rispetto del quadro ordinamentale di riferimento, nei limiti delle facoltà assunzionali delle amministrazioni interessate, senza nuovi o maggiori oneri per il bilancio dello Stato e senza determinare posizioni sovrannumerarie e riconoscimento di differenziali economici ».

PROPOSTE EMENDATIVE

ART. 12.

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

Sopprimerlo.

12.1. Pastorella.

Al comma 1, alinea, sostituire le parole: sono aggiunti i seguenti *con le seguenti:* è aggiunto il seguente.

*Conseguentemente, al comma 1, sopprimere il capoverso 8-*quater.

12.200. Le Commissioni.

(Approvato)

*Al comma 1, capoverso comma 8-*ter*, primo periodo, sostituire le parole da:* per la durata di due anni *fino a:* percorsi formativi *con le seguenti:* della durata complessiva di almeno un anno, salvo specifica autorizzazione da parte dell'Agenzia,

Conseguentemente al medesimo comma, medesimo capoverso:

al medesimo periodo, aggiungere, in fine, le parole: per il successivo anno a decorrere dalla data di completamento di ciascuno dei predetti percorsi formativi.

al terzo periodo, dopo le parole: Le disposizioni del presente comma non si applicano *aggiungere le seguenti:* al personale a tempo determinato ai sensi del decreto del Presidente del Consiglio dei ministri n. 224 del 2021 proveniente direttamente dai ruoli delle Forze armate e delle Forze di polizia ad ordinamento civile e militare di cui all'articolo 16 della legge 1° aprile 1981, n. 121, nonché.

12.102. Mauri, Bonafè, Cuperlo, Fornaro, Gianassi, Serracchiani, Di Biase, Zan, Lacarra, Casu.

Al comma 1, capoverso comma 8-*quater, primo periodo, sostituire le parole:* di cui ai commi 8 e 8.1 dell'articolo 17, entrato *aggiungere la seguente:* immesso.

Conseguentemente, al medesimo comma, medesimo capoverso:

al secondo periodo, sopprimere le parole : All'attuazione delle disposizioni del primo periodo*„;*

al terzo periodo:

dopo le parole: si applicano *aggiungere le seguenti:* a decorrere dalla data di costituzione dell'Agenzia*;*

sopprimere le parole : e senza determinare posizioni sovrannumerarie e riconoscimento di differenziali economici.

12.100. Boschi.

Dopo il comma 1, aggiungere il seguente:

2. Fino al 31 dicembre 2026, per il personale dell'Agenzia per la cybersicurezza nazionale il requisito di permanenza minima nell'Area operativa ai fini del passaggio all'Area manageriale e alte professionalità è fissato in tre anni.

12.101. Pulciani, Mollicone.

(Approvato)

Dopo l'articolo 12, aggiungere il seguente:

Art. 12-*bis*.

(Disposizioni in materia di personale degli Organismi di informazione per la sicurezza)

1. Coloro che hanno ricoperto la carica di Direttore generale e di Vice Direttore generale del DIS e di Direttore e di Vice Direttore di AISE o di AISI, ovvero abbiano svolto incarichi dirigenziali di prima fascia di preposizione a strutture organizzative di livello dirigenziale generale non possono, salvo autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità Delegata ove istituita, nei tre anni successivi alla cessazione dell'incarico svolgere attività lavorativa, professionale, o consulenziale, ovvero ricoprire cariche presso soggetti esteri, pubblici o privati, ovvero presso soggetti privati italiani a cui si applica il decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56. L'autorizzazione è concessa avuto riguardo alle esigenze di protezione e di tutela del patrimonio informativo acquisito durante l'espletamento dell'incarico, e alla necessità di evitare comunque pregiudizi per la sicurezza nazionale.

2. Il personale di cui al ruolo unico previsto dall'articolo 21 della legge 3 agosto 2007, n. 124, non può, nei tre anni successivi alla

cessazione dal servizio presso il DIS, l'AISE e l'AISI, svolgere attività lavorativa, professionale o consulenziale, ovvero ricoprire cariche, presso enti o privati titolari di licenza ai sensi dell'articolo 134 del TULPS, o comunque presso soggetti che a qualunque titolo svolgano attività di investigazione, ricerca o raccolta informativa.

3. Il personale di cui al ruolo unico previsto dall'articolo 21 della legge 3 agosto 2007, n. 124, che abbia partecipato, nell'interesse e a spese del DIS, dell'AISE o dell'AISI, a specifici percorsi formativi di specializzazione, non può essere assunto, né assumere incarichi presso soggetti privati per svolgere le medesime mansioni per le quali ha beneficiato delle suddette attività formative, per la durata di tre anni a decorrere dalla data di completamento dell'ultimo dei predetti percorsi formativi.

4. I contratti conclusi e gli incarichi conferiti in violazione dei divieti di cui al presente articolo sono nulli.

5. Con regolamento adottato ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124, sono definiti le procedure di autorizzazione per i casi di cui al comma 1, gli obblighi di dichiarazione e di comunicazione a carico dei dipendenti, i casi in cui non si applicano i divieti di cui ai commi 2 e 3, le modalità di individuazione dei percorsi formativi che determinano il divieto di cui al comma 3.

12.0100. Pulciani, Mollicone.

(Approvato)

A.C. 1717-A – Articolo 13

ARTICOLO 13 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI

Art. 13.

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

1. Con decreto del Presidente del Consiglio dei ministri, da adottare entro centoventi giorni dalla data di entrata in vigore della presente legge, su proposta dell'Agenzia per la cybersicurezza nazionale, previo parere del Comitato interministeriale per la sicurezza della Repubblica, di cui all'articolo 5 della legge 3 agosto 2007, n. 124, nella composizione di cui all'articolo 10, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, sono individuati, per specifiche categorie tecnologiche di beni e servizi informatici, gli elementi essenziali di cybersicurezza che i soggetti di cui all'articolo 2, comma 2, del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, tengono in considerazione nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici nonché i casi in cui, per la tutela della sicurezza nazionale, devono essere previsti criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO). Ai fini del presente articolo, per « elementi essenziali di cybersicurezza » si intende l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela di cui al primo periodo.

2. Nei casi individuati ai sensi del comma 1, le stazioni appaltanti, comprese le centrali di committenza:

a) possono esercitare la facoltà di cui agli articoli 107, comma 2, e 108, comma 10, del codice dei contratti pubblici, di cui al decreto legislativo 31 marzo 2023, n. 36, se accertano che l'offerta non tiene in considerazione gli elementi essenziali di cybersicurezza individuati con il decreto di cui al comma 1;

b) tengono sempre in considerazione gli elementi essenziali di cybersicurezza di cui al comma 1 nella valutazione dell'elemento qualitativo, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione;

c) nel caso in cui sia utilizzato il criterio del minor prezzo, ai sensi dell'articolo 108, comma 3, del codice di cui al decreto legislativo n. 36 del 2023, inseriscono gli elementi di cybersicurezza di cui al comma 1 tra i requisiti minimi dell'offerta;

d) nel caso in cui sia utilizzato il criterio dell'offerta economicamente più vantaggiosa, ai sensi dell'articolo 108, comma 4, del codice di cui al decreto legislativo n. 36 del 2023, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del migliore rapporto qualità/prezzo, stabiliscono un tetto massimo per il punteggio economico entro il limite del 10 per cento.

e) prevedono criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti alla NATO, al fine di tutelare la sicurezza nazionale e di conseguire l'autonomia tecnologica e strategica nell'ambito della cybersicurezza.

3. Le disposizioni di cui al comma 1 si applicano anche ai soggetti privati non compresi fra quelli di cui all'articolo 2, comma 2, del codice di cui al decreto legislativo 7 marzo 2005, n. 82, e inclusi nell'elencazione di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

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

PROPOSTE EMENDATIVE

ART. 13.

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

Al comma 1, primo periodo, dopo le parole: di Paesi appartenenti all'Unione europea *aggiungere le seguenti:* o di Paesi terzi associati ai programmi dell'Unione europea in materia di ricerca e innovazione.

Conseguentemente, al comma 2, lettera e)*, dopo le parole:* di Paesi aderenti all'Unione europea *aggiungere le seguenti:* o di Paesi terzi associati ai programmi dell'Unione europea in materia di ricerca e innovazione.

13.101. Orsini.

Al comma 1, primo periodo, dopo le parole: aderenti all'Alleanza atlantica (NATO) *aggiungere le seguenti:* o di Paesi terzi individuati con il decreto di cui al presente comma tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

Conseguentemente, al comma 2, lettera e)*, dopo le parole:* Paesi aderenti alla NATO *aggiungere le seguenti:* o di Paesi terzi individuati con il decreto di cui al comma 1 tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

13.101. *(Testo modificato nel corso della seduta)* Orsini.

(Approvato)

Al comma 1, primo periodo, dopo le parole: aderenti all'Alleanza atlantica (NATO) *aggiungere le seguenti:* o che hanno sottoscritto con quest'ultima accordi di collaborazione in materia di cybersicurezza o di protezione delle informazioni classificate;

Conseguentemente, al comma 2, lettera e), *dopo le parole :* Paesi aderenti alla NATO *aggiungere le seguenti:* o che hanno sottoscritto con quest'ultima accordi di collaborazione in materia di cybersicurezza o di protezione delle informazioni classificate.

13.102. Gardini, Mollicone, Urzì.

Al comma 1, primo periodo, dopo le parole: aderenti all'Alleanza atlantica (NATO) *aggiungere le seguenti:* o di Paesi terzi individuati con il decreto di cui al presente comma tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

Conseguentemente, al comma 2, lettera e), *dopo le parole:* Paesi aderenti alla NATO *aggiungere le seguenti:* o di Paesi terzi individuati con il decreto di cui al comma 1 tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

13.102. *(Testo modificato nel corso della seduta)* Gardini, Mollicone, Urzì.

(Approvato)

Al comma 1, primo periodo, dopo le parole: aderenti all'Alleanza atlantica (NATO) *aggiungere le seguenti:* o di Paesi con i quali lo Stato italiano abbia sottoscritto accordi di cooperazione nell'ambito della sicurezza o della sicurezza informatica.

Conseguentemente, al comma 2, lettera e), *dopo le parole :* Paesi aderenti alla NATO *aggiungere le seguenti:* o di Paesi con i quali lo Stato italiano abbia sottoscritto accordi di cooperazione nell'ambito della sicurezza o della sicurezza informatica.

13.103. Rosato.

Al comma 1, primo periodo, dopo le parole: aderenti all'Alleanza atlantica (NATO) *aggiungere le seguenti: o* di Paesi terzi individuati con il decreto di cui al presente comma tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

Conseguentemente, al comma 2, lettera e), *dopo le parole:* Paesi aderenti alla NATO *aggiungere le seguenti: o* di Paesi terzi individuati con il decreto di cui al comma 1 tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

13.103. *(Testo modificato nel corso della seduta)* Rosato.

(Approvato)

Al comma 1, aggiungere, in fine, i seguenti periodi: Tali specifici requisiti di sicurezza tecnologica sono indipendenti dalla provenienza geografica delle aziende partecipanti ai bandi. Nell'adozione del decreto di cui al presente comma, ai fini dell'individuazione degli elementi essenziali di cybersicurezza, si tiene conto altresì di quanto previsto dalla normativa europea di riferimento in termini di criteri riferiti a prodotti e servizi di cybersicurezza acquisiti dalla Pubblica Amministrazione mediante contratti pubblici e, laddove disponibili, si prediligono le certificazioni europee in materia di sicurezza cibernetica previste dal Regolamento (UE) 2019/881 (Regolamento sulla Cybersicurezza).

13.5. Pastorella.

Dopo l'articolo 13, aggiungere il seguente:

Art. 13-*bis*.

(Esclusione di applicabilità di talune sanzioni di cui al decreto legislativo 1° agosto 2003, n. 259)

1. All'articolo 57 del decreto legislativo 1° agosto 2003, n. 259 , dopo il comma 9, è aggiunto il seguente:

« 9-*bis*. I soggetti obbligati di cui al presente articolo non sono responsabili delle comunicazioni criptate nei casi in cui:

a) i servizi di comunicazione sono forniti da terze parti;

b) non dispongono degli strumenti per decifrare le comunicazioni criptate effettuate attraverso applicazioni o sistemi utilizzati autonomamente dall'utente;

c) la tecnologia al momento disponibile non consente tecnicamente la messa in chiaro della comunicazione. »

13.02. Casu, Bonafè, Cuperlo, Fornaro, Mauri, Gianassi, Serracchiani, Di Biase, Lacarra, Zan.

A.C. 1717-A – Articolo 14

ARTICOLO 14 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI

Art. 14.

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

1. All'articolo 16, comma 2, della legge 21 febbraio 2024, n. 15, dopo la lettera *c)* è inserita la seguente:

« *c-bis)* apportare alla disciplina applicabile agli intermediari finanziari iscritti nell'albo previsto dall'articolo 106 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, nonché alla società Poste italiane Spa per l'attività del Patrimonio Bancoposta, di cui al regolamento di cui al decreto del Presidente della Repubblica 14 marzo 2001, n. 144, le occorrenti modifiche e integrazioni, anche mediante la normativa secondaria di cui alla lettera *d)* del presente comma, per conseguire un livello elevato di resilienza operativa digitale e assicurare la stabilità del settore finanziario nel suo complesso, in particolare:

1) definendo presìdi in materia di resilienza operativa digitale equivalenti a quelli stabiliti nel regolamento (UE) 2022/2554;

2) tenendo conto, nella definizione dei presìdi di cui al numero 1), del principio di proporzionalità e delle attività svolte dagli intermediari finanziari e dal Patrimonio Bancoposta;

3) attribuendo alla Banca d'Italia l'esercizio nei confronti dei soggetti di cui alla presente lettera dei poteri di vigilanza, di indagine e sanzionatori di cui alla lettera *b)* ».

A.C. 1717-A – Articolo 15

ARTICOLO 15 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI

CAPO II

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

Art. 15.

(Modifiche al codice penale)

1. Al codice penale sono apportate le seguenti modificazioni:

a) all'articolo 240, secondo comma, numero 1-*bis*, dopo la parola: « 635-*quin-*

quies, » sono inserite le seguenti: « 640, secondo comma, numero 2-*ter*), »;

b) all'articolo 615-*ter*:

1) al secondo comma:

1.1) all'alinea, le parole: « da uno a cinque anni » sono sostituite dalle seguenti: « da due a dieci anni »;

1.2) al numero 2), dopo la parola: « usa » sono inserite le seguenti: « minaccia o »;

1.3) al numero 3), dopo le parole: « ovvero la distruzione o il danneggiamento » sono inserite le seguenti: « ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare »;

2) al terzo comma, le parole: « da uno a cinque anni e da tre a otto anni » sono sostituite dalle seguenti: « da tre a dieci anni e da quattro a dodici anni »;

c) all'articolo 615-*quater*:

1) al primo comma, la parola: « profitto » è sostituita dalla seguente: « vantaggio »;

2) il secondo comma è sostituito dal seguente:

« La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-*ter*, secondo comma, numero 1) »;

3) dopo il secondo comma è aggiunto il seguente:

« La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-*ter*, terzo comma »;

d) l'articolo 615-*quinquies* è abrogato;

e) all'articolo 617-*bis*:

1) dopo il primo comma è inserito il seguente:

« La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-*ter*, secondo comma, numero 1) »;

2) al secondo comma, le parole: « ovvero da un pubblico ufficiale » fino alla fine del comma sono soppresse;

f) all'articolo 617-*quater*, quarto comma:

1) all'alinea, le parole: « da tre a otto anni » sono sostituite dalle seguenti: « da quattro a dieci anni »;

2) il numero 1) è sostituito dal seguente:

« 1) in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615-*ter*, terzo comma »;

3) al numero 2), le parole: « da un pubblico ufficiale » sono sostituite dalle seguenti: « in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o da un pubblico ufficiale » e la parola: « ovvero » è sostituita dalle seguenti: « o da chi esercita, anche abusivamente, la professione di investigatore privato, o »;

4) il numero 3) è abrogato;

g) all'articolo 617-*quinquies*:

1) il secondo comma è sostituito dal seguente:

« Quando ricorre taluna delle circostanze di cui all'articolo 617-*quater*, quarto comma, numero 2), la pena è della reclusione da due a sei anni »;

2) dopo il secondo comma è aggiunto il seguente:

« Quando ricorre taluna delle circostanze di cui all'articolo 617-*quater*, quarto comma, numero 1), la pena è della reclusione da tre a otto anni ».

h) all'articolo 617-*sexies*, secondo comma, le parole: « da uno a cinque anni » sono sostituite dalle seguenti: « da tre a otto anni »;

i) nella rubrica del capo III-*bis* del titolo XII del libro secondo, le parole: « sulla procedibilità » sono soppresse;

l) dopo l'articolo 623-*ter* è inserito il seguente:

« Art. 623-*quater*. – *(Circostanze attenuanti)* – Le pene comminate per i delitti di

cui agli articoli 615-*ter*, 615-*quater*, 617-*quater*, 617-*quinquies* e 617-*sexies* sono diminuite quando, per la natura, la specie, i mezzi, le modalità o circostanze dell'azione ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità.

Le pene previste per i delitti di cui al primo comma sono diminuite dalla metà a due terzi per chi si adopera per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi.

Non si applica il divieto di cui all'articolo 69, quarto comma »;

m) all'articolo 629, dopo il secondo comma è aggiunto il seguente:

« Chiunque, mediante le condotte di cui agli articoli 615-*ter*, 617-*quater*, 617-*sexies*, 635-*bis*, 635-*quater* e 635-*quinquies* ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nell'ultimo capoverso dell'articolo precedente »;

n) all'articolo 635-*bis*:

1) al primo comma, le parole: « da sei mesi a tre anni » sono sostituite dalle seguenti: « da due a sei anni »;

2) il secondo comma è sostituito dal seguente:

« La pena è della reclusione da tre a otto anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato »;

o) all'articolo 635-*ter*:

1) al primo comma, le parole: « utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni » sono sostituite dalle seguenti: « di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, è punito con la reclusione da due a sei anni »;

2) il secondo e il terzo comma sono sostituiti dai seguenti:

« La pena è della reclusione da tre a otto anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.

La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3) »;

3) nella rubrica, le parole: « utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità » sono sostituite dalle seguenti: « pubblici o di interesse pubblico »;

p) all'articolo 635-*quater*:

1) al primo comma, le parole: « da uno a cinque anni » sono sostituite dalle seguenti: « da due a sei anni »;

2) il secondo comma è sostituito dal seguente:

« La pena è della reclusione da tre a otto anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato »;

q) dopo l'articolo 635-*quater* è inserito il seguente:

« *Art. 635-quater.1. – (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)* – Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici è punito con la reclusione fino a due anni e con la multa fino a euro 10.329.

La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-*ter*, secondo comma, numero 1).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-*ter*, terzo comma »;

r) l'articolo 635-*quinquies* è sostituito dal seguente:

« *Art. 635-quinquies. – (Danneggiamento di sistemi informatici o telematici di pubblico interesse)* – Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-*bis* ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, compie atti diretti a distruggere, danneggiare o rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento è punito con la pena della reclusione da due a sei anni.

La pena è della reclusione da tre a otto anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.

La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3) »;

s) dopo l'articolo 639-*bis* è inserito il seguente:

« Art. 639-*ter*. – *(Circostanze attenuanti)* – Le pene comminate per i delitti di cui agli articoli 629, terzo comma, 635-*ter*, 635-*quater*.1 e 635-*quinquies* sono diminuite quando per la natura, la specie, i mezzi, le modalità o circostanze dell'azione, ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità.

Le pene comminate per i delitti di cui al primo comma sono diminuite dalla metà a due terzi per chi si adopera per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel recu-

pero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi.

Non si applica il divieto di cui all'articolo 69, quarto comma ».

t) all'articolo 640:

1) al secondo comma è aggiunto, in fine, il seguente numero:

« 2-*ter*) se il fatto è commesso a distanza attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione »;

2) al terzo comma, le parole: « capoverso precedente » sono sostituite dalle seguenti: « secondo comma, a eccezione di quella di cui al numero 2-*ter*) »;

u) all'articolo 640-*quater*, le parole: « numero 1 » sono sostituite dalle seguenti: « numeri 1 e 2-*ter*) ».

PROPOSTE EMENDATIVE

ART. 15.

(Modifiche al codice penale)

Al comma 1, alla lettera a), *premettere la seguente:*

0a) all'articolo 52, secondo comma:

1) dopo le parole: « Nei casi previsti dall'articolo 614, primo e secondo comma » sono aggiunte le seguenti: « , nonché dagli articoli 615-*ter*, 615-*quater*, 615-*quinquies*, 635-*bis*, 635-*quater*, 635-*quater*.1, »;

2) dopo le parole: « usa un'arma legittimamente detenuta o altro mezzo » sono aggiunte le seguenti: « , anche informatico, ».

15.4. Casu, Gianassi, Serracchiani, Di Biase, Zan, Lacarra, Bonafè, Mauri, Cuperlo, Fornaro, Boschi.

Al comma 1, lettera c), *sopprimere il numero 1).*

15.12. Enrico Costa.

Al comma 1, sostituire la lettera m) con la seguente:

m) all'articolo 629:

1. al secondo comma, le parole « nell'ultimo capoverso dell'articolo precedente » sono sostituite dalle seguenti: « nel terzo comma dell'articolo 628 »;

2. dopo il secondo comma è aggiunto il seguente:

« Chiunque, mediante le condotte di cui agli articoli 615-*ter*, 617-*quater*, 617-*sexies*, 635-*bis*, 635-*quater* e 635-*quinquies*, ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628. ».

15.100. Pulciani.

(Approvato)

Al comma 1, lettera m), *capoverso, secondo periodo, sostituire le parole:* nell'ultimo capoverso dell'articolo precedente *con le seguenti:* nel terzo comma dell'articolo 628, nonché nel caso in cui il fatto sia commesso nei confronti di minori o disabili.

15.24. D'Orso, Ascari, Cafiero De Raho, Giuliano, Alfonso Colucci, Alifano, Auriemma, Penza.

Al comma 1, lettera m), *capoverso, secondo periodo, sostituire le parole:* nell'ultimo capoverso dell'articolo precedente *con le seguenti:* nel terzo comma dell'articolo 628, nonché nel caso in cui il fatto sia commesso nei confronti di incapaci per età o per infermità.

15.24. *(Testo modificato nel corso della seduta)* D'Orso, Ascari, Cafiero De Raho,

Giuliano, Alfonso Colucci, Alifano, Auriemma, Penza.

(Approvata limitatamente alla parte non assorbita per effetto dell'approvazione dell'emendamento Pulciani 15.100)

Al comma 1, aggiungere, in fine, la seguente lettera:

v) all'articolo 640-*quinquies*, le parole: « fino a tre anni » sono sostituite dalle seguenti: « da due a cinque anni » e le parole: « da 51 a 1.032 euro » sono sostituite dalle seguenti: « da 500 a 5.000 euro ».

15.32. D'Orso, Ascari, Cafiero De Raho, Giuliano, Alfonso Colucci, Alifano, Auriemma, Penza.

A.C. 1717-A – Articolo 16

ARTICOLO 16 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI IDENTICO A QUELLO DEL GOVERNO

Art. 16.

(Modifiche al codice di procedura penale)

1. Al codice di procedura penale sono apportate le seguenti modificazioni:

a) all'articolo 51, comma 3-*quinquies*:

1) la parola: « 615-*quinquies*, » è soppressa;

2) dopo la parola: « 635-*quater*, » sono inserite le seguenti: « 635-*quater*.1, 635-*quinquies*, »;

3) dopo le parole: « del codice penale, » sono inserite le seguenti: « o per il delitto di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, »;

b) all'articolo 406, comma 5-*bis*, le parole: « numeri 4 e 7-*bis* » sono sostituite dalle seguenti: « numeri 4), 7-*bis*) e 7-*ter*) »;

c) all'articolo 407, comma 2, lettera *a)*, dopo il numero 7-*bis*) è aggiunto il seguente:

« 7-*ter*) delitti previsti dagli articoli 615-*ter*, 615-*quater*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, 635-*quater*.1 e 635-*quinquies* del codice penale, quando il fatto è commesso in danno di sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico ».

PROPOSTE EMENDATIVE

ART. 16.

(Modifiche al codice di procedura penale)

Al comma 1, alla lettera a), *premettere la seguente*:

0a) all'articolo 8, è aggiunto, in fine, il seguente comma:

« 4-*bis*. Se si tratta di reati informatici, la competenza è del giudice del luogo dove si trova il sistema informatico ».

16.1. D'Orso, Ascari, Cafiero De Raho, Giuliano, Alfonso Colucci, Alifano, Auriemma, Penza.

Al comma 1, lettera a), *al numero 1), premettere, il seguente:*

01) dopo le parole: « di cui agli articoli 414-*bis*, » sono aggiunte le seguenti: « 493-*ter*, 493-*quater*, »

16.4. D'Orso, Ascari, Cafiero De Raho, Giuliano, Alfonso Colucci, Alifano, Auriemma, Penza.

Al comma 1, lettera a), *sostituire il numero 2) con il seguente:*

2) le parole: « 635-*bis*, 635-*ter*, 635-*quater* » sono sostituite dalle seguenti: « 629,

635-*bis*, 635-*ter*, 635-*quater*, 635-*quater*.1, 635-*quinquies*, ».

16.3. D'Orso, Ascari, Cafiero De Raho, Giuliano, Alfonso Colucci, Alifano, Auriemma, Penza.

Al comma 1, lettera a), *numero 3), aggiungere, in fine, le parole:* , nonché nei casi di cui agli articoli 167, 167-*bis* e 167-*ter* del Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

16.5. D'Orso, Ascari, Cafiero De Raho, Giuliano, Alfonso Colucci, Alifano, Auriemma, Penza.

Al comma 1, dopo la lettera a), *aggiungere la seguente*:

a-bis) all'articolo 371-*bis*, comma 1, primo periodo, sono aggiunte, in fine, le parole: « nonché di contrasto alla criminalità informatica ».

16.9. D'Orso, Ascari, Cafiero De Raho, Giuliano, Alfonso Colucci, Alifano, Auriemma, Penza.

Dopo l'articolo 16, aggiungere il seguente:

Art. 16-*bis*.

(Competenza territoriale in materia di reati informatici)

1. Per i procedimenti penali per i reati di cui alla presente legge è competente il giudice distrettuale del luogo in cui si trova il sistema informatico.

2. Nei casi in cui si tratti di più sistemi informatici coinvolti nel reato si applica l'articolo 9, comma 3, del codice di procedura penale.

16.02. Gianassi, Serracchiani, Di Biase, Zan, Lacarra, Bonafè, Mauri, Cuperlo, Fornaro.

A.C. 1717-A – Articolo 17

ARTICOLO 17 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI IDENTICO A QUELLO DEL GOVERNO

Art. 17.

(Modifiche al decreto-legge 15 gennaio 1991, n. 8, convertito, con modificazioni, dalla legge 15 marzo 1991, n. 82)

1. Al decreto-legge 15 gennaio 1991, n. 8, convertito, con modificazioni, dalla legge 15 marzo 1991, n. 82, sono apportate le seguenti modificazioni:

a) all'articolo 9, comma 2, dopo le parole: « 51, comma 3-*bis*, » sono inserite le seguenti: « o all'articolo 371-*bis*, comma 4-*bis*, »;

b) all'articolo 11, comma 2, dopo le parole: « 51, commi 3-*bis* e 3-*quater*, » sono inserite le seguenti: « o all'articolo 371-*bis*, comma 4-*bis*, »;

c) all'articolo 16-*novies*, comma 1, dopo le parole: « 51, comma 3-*bis*, » sono inserite le seguenti: « o all'articolo 371-*bis*, comma 4-*bis*, ».

A.C. 1717-A – Articolo 18

ARTICOLO 18 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI IDENTICO A QUELLO DEL GOVERNO

Art. 18.

(Modifica al decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203)

1. All'articolo 13 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, dopo il comma 3 è aggiunto il seguente:

« *3-bis*. Le disposizioni dei commi 1, 2 e 3 si applicano anche quando si procede in relazione a taluno dei delitti, consumati o ten-

tati, previsti dall'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale ».

PROPOSTE EMENDATIVE

ART. 18.

(Modifica al decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203)

Sopprimerlo

18.1. Enrico Costa.

Dopo l'articolo 18 aggiungere il seguente:

Art. 18-*bis*.

(Modifiche al decreto legislativo 30 giugno 2003 n. 196)

1. All'articolo 167, al comma 4, del decreto legislativo 30 giugno 2003 n. 196, dopo le parole: « reati di cui ai commi 1, 2 e 3, » sono inserite le seguenti: « nonché nei casi previsti dagli articoli 615-*ter*, 615-*quater*, 615-*quinquies*, 635-*bis*, 635-*quater*, 635-*quater*.1, ».

18.01. Gianassi, Serracchiani, Di Biase, Zan, Lacarra, Bonafè, Mauri, Cuperlo, Fornaro.

Dopo l'articolo 18, aggiungere il seguente:

Art. 18-*bis*.

(Modifiche al decreto legislativo 30 giugno 2003, n. 196 del Codice in materia di protezione dei dati personali)

1. All'articolo 167-*ter*, comma 1, del decreto legislativo 30 giugno 2003, n. 196, recante Codice in materia di protezione dei dati personali, le parole: « da uno a quattro » sono sostituite dalle seguenti: « da due a sei »;.

18.02. D'Orso, Ascari, Cafiero De Raho, Giuliano, Alfonso Colucci, Alifano, Auriemma, Penza.

A.C. 1717-A – Articolo 19

ARTICOLO 19 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI IDENTICO A QUELLO DEL GOVERNO

Art. 19.

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

1. All'articolo 24-*bis* del decreto legislativo 8 giugno 2001, n. 231, sono apportate le seguenti modificazioni:

a) al comma 1, le parole: « da cento a cinquecento quote » sono sostituite dalle seguenti: « da duecento a settecento quote »;

b) dopo il comma 1 è inserito il seguente:

« *1-bis*. In relazione alla commissione del delitto di cui all'articolo 629, terzo comma, del codice penale, si applica all'ente la sanzione pecuniaria da trecento a ottocento quote »;

c) al comma 2, la parola: « 615-*quinquies* » è sostituita dalla seguente: « 635-*quater*.1 » e le parole: « sino a trecento quote » sono sostituite dalle seguenti: « sino a quattrocento quote »;

d) al comma 4, dopo il primo periodo è inserito il seguente: « Nei casi di condanna per il delitto indicato nel comma 1-*bis* si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a due anni ».

A.C. 1717-A – Articolo 20

ARTICOLO 20 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI IDENTICO A QUELLO DEL GOVERNO

Art. 20.

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

1. All'articolo 11, comma 2, della legge 11 gennaio 2018, n. 6, dopo le parole: « 51,

commi 3-*bis*, 3-*ter* e 3-*quater*, » sono inserite le seguenti: « o all'articolo 371-*bis*, comma 4-*bis*, ».

A.C. 1717-A – Articolo 21

ARTICOLO 21 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI IDENTICO A QUELLO DEL GOVERNO

Art. 21.

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

1. All'articolo 17 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, sono apportate le seguenti modificazioni:

a) il comma 4 è sostituito dal seguente:

« *4*. Il personale dell'Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni, riveste la qualifica di pubblico ufficiale. La trasmissione immediata 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 »;

b) dopo il comma 4-*bis* sono inseriti i seguenti:

« *4-bis.1*. Nei casi in cui l'Agenzia ha notizia di un attacco ai danni di uno dei sistemi informatici o telematici di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale e in ogni caso quando risulti interessato taluno dei soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, di cui all'articolo 3, comma 1, lettere *g)* e *i)*, del decreto legislativo 18 maggio 2018, n. 65, ovvero di cui all'articolo 40, comma 3, alinea, del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259, fermo restando quanto previsto dal comma 4 del presente articolo, procede alle attività di cui all'articolo 7, comma 1, lettere *n)* e *n-bis)*, e ne informa senza ritardo il procuratore nazionale antimafia e antiterrorismo, ai sensi del comma 4-*bis*;

4-bis.2. Fuori dei casi di cui al comma 4-*bis*.1, quando acquisisce la notizia dei delitti di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale, il pubblico ministero ne dà tempestiva informazione all'Agenzia e assicura, altresì, il raccordo informativo con l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione ai fini di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

4-bis.3. In ogni caso, il pubblico ministero impartisce le disposizioni necessarie ad assicurare che gli accertamenti urgenti siano compiuti tenendo conto delle attività svolte dall'Agenzia, a fini di resilienza, di cui all'articolo 7, comma 1, lettere *n)* e *n-bis)*, e può disporre il differimento di una o più delle predette attività, con provvedimento motivato adottato senza ritardo, per evitare un grave pregiudizio per il corso delle indagini.

4-bis.4. Il pubblico ministero, quando procede ad accertamenti tecnici irripetibili in relazione ai delitti di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale, informa senza ritardo l'Agenzia, che mediante propri rappresentanti può assistere al conferimento dell'incarico e partecipare agli accertamenti. Le disposizioni del primo periodo si applicano anche quando agli accertamenti si procede nelle forme dell'incidente probatorio ».

A.C. 1717-A – Articolo 22

ARTICOLO 22 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI

Art. 22.

(Modifiche all'articolo 7 della legge 12 agosto 1962, n. 1311)

1. All'articolo 7 della legge 12 agosto 1962, n. 1311, sono apportate le seguenti modificazioni:

a) al primo comma è aggiunto, in fine, il seguente periodo: « Nelle ispezioni è verificato altresì il rispetto delle prescrizioni di sicurezza negli accessi alle banche di dati in uso presso gli uffici giudiziari »;

b) al terzo comma, le parole: « degli stessi nonché » sono sostituite dalle seguenti: « degli stessi, » e sono aggiunte, in fine, le seguenti parole: « nonché il rispetto delle prescrizioni di sicurezza negli accessi alle banche di dati in uso presso gli uffici giudiziari ».

PROPOSTE EMENDATIVE

ART. 22.

(Modifiche all'articolo 7 della legge 12 agosto 1962, n. 1311)

Sopprimerlo.

*** 22.100.** Dori, Zaratti.

Sopprimerlo.

*** 22.102.** Gianassi, Serracchiani, Di Biase, Lacarra, Zan, Bonafè, Cuperlo, Fornaro, Mauri.

Sopprimerlo.

*** 22.101.** D'Orso, Ascari, Cafiero De Raho, Giuliano.

A.C. 1717-A – Articolo 23

ARTICOLO 23 DEL DISEGNO DI LEGGE NEL TESTO DELLE COMMISSIONI IDENTICO A QUELLO DEL GOVERNO

Art. 23.

(Disposizioni finanziarie)

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

2. I proventi delle sanzioni di cui all'articolo 1, comma 5, confluiscono nelle entrate dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 11, comma 2, lettera *f)*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

PROPOSTE EMENDATIVE

ART. 23.

(Disposizioni finanziarie)

Sopprimere il comma 1.

23.1. Bonafè, Mauri, Cuperlo, Fornaro, Casu, Serracchiani, Di Biase, Zan, Lacarra, Gianassi.

Sostituire il comma 1 con il seguente:

1. Presso il Ministero dell'economia e delle finanze è istituito un Fondo per la sicurezza informatica, per l'attuazione delle disposizioni di cui alla presente legge, cui confluiscono le risorse annualmente stanziate dalla legge di bilancio per un importo comunque non inferiore all'1,2 per cento degli investimenti nazionali lordi. Il Ministro dell'economia e delle finanze con proprio decreto, sulla base delle risorse rese

disponibili annualmente ai sensi del presente comma, assegna lo stanziamento a favore dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 11, comma 2, lettera *f)*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

23.3. Bonafè, Mauri, Cuperlo, Fornaro, Casu, Serracchiani, Di Biase, Zan, Lacarra, Gianassi.

Sostituire il comma 1 con il seguente:

1. Agli oneri derivanti dall'attuazione della presente legge, pari a 100 milioni di euro per ciascuno degli anni 2024 e 2025, si provvede mediante corrispondente riduzione del Fondo per interventi strutturali di politica economica di cui all'articolo 10, comma 5, del decreto-legge 29 novembre 2004, n. 282, convertito, con modificazioni, dalla legge 27 dicembre 2004, n. 307.

23.4. Bonafè, Mauri, Cuperlo, Fornaro, Serracchiani, Di Biase, Zan, Lacarra, Gianassi, Casu.

Al comma 2, dopo le parole: comma 5, *aggiungere le seguenti:* nonché le risorse derivanti dai ribassi d'asta relativi agli interventi ad ogni titolo rientranti fra i progetti PNRR di titolarità delle amministrazioni centrali,.

23.5. Bonafè, Mauri, Cuperlo, Fornaro, Casu, Serracchiani, Di Biase, Zan, Lacarra, Gianassi.

Al comma 2, sostituire le parole da: confluiscono nelle entrate *fino alla fine del comma, con le seguenti:* sono versati in apposito capitolo di entrata del bilancio dello Stato per essere riassegnati allo stato di previsione della spesa del Ministero dell'economia e delle finanze a favore per il 50 per cento all'Agenzia per la Cybersicurezza nazionale ai sensi all'articolo 11, comma 2, lettera *f)*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, e per la restante parte al Fondo di cui all'articolo 239 del decreto-legge 19 maggio 2020, n. 34, convertito, con modificazioni, dalla legge 17 luglio 2020, n. 77.

23.11. Auriemma, Alfonso Colucci, Alifano, Penza, D'Orso, Ascari, Cafiero De Raho, Giuliano.

Dopo il comma 2 aggiungere i seguenti:

3. Presso il Ministero dell'economia e delle finanze è istituito un Fondo per la sicurezza informatica, cui confluiscono le risorse derivanti dai ribassi d'asta relativi agli interventi ad ogni titolo rientranti fra i progetti PNRR di titolarità delle amministrazioni centrali.

4. Il Ministro dell'economia e delle finanze con proprio decreto, sulla base delle risorse rese disponibili annualmente ai sensi del comma 2-*bis*, assegna lo stanziamento a favore dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 11, comma 2, lettera *f)*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109 per la copertura degli eventuali oneri derivanti dall'attuazione della presente legge e la realizzazione degli scopi istituzionali alla medesima assegnati.

23.12. Casu, Bonafè, Cuperlo, Fornaro, Mauri, Serracchiani, Di Biase, Zan, Lacarra, Gianassi.

Dopo il comma 2 aggiungere i seguenti:

3. Presso il Ministero dell'economia e delle finanze è istituito un Fondo per la sicurezza informatica, cui confluiscono le risorse annualmente stanziate dalla legge di bilancio per un importo comunque non inferiori all'1,2 per cento degli investimenti nazionali lordi.

4. Il Ministro dell'economia e delle finanze con proprio decreto, sulla base delle risorse rese disponibili annualmente ai sensi del comma 2-*bis* assegna lo stanziamento a favore dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 11, comma 2, lettera *f)*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109 per la copertura degli eventuali oneri derivanti dall'attua-

zione della presente legge e la realizzazione degli scopi istituzionali alla medesima assegnati.

23.13. Casu, Bonafè, Cuperlo, Fornaro, Mauri, Serracchiani, Di Biase, Zan, Lacarra, Gianassi.

A.C. 1717-A – Ordini del giorno

ORDINI DEL GIORNO

La Camera,

premesso che

le informazioni riguardanti il settore agroalimentare nazionale assumono una rilevanza centrale nell'ambito della tutela della salute pubblica e del *Made in Italy*;

nel quadro del rafforzamento della cybersicurezza nazionale emerge la necessità di inserire strumenti idonei a garantire a tutela delle attività di raccolta e conservazione dei dati afferenti al comparto agricolo e alimentare nazionale;

all'evidenza dei fatti, mostrata anche dal ripetersi degli attacchi *hacker* da parte di criminali informatici alle reti OT a società ed enti pubblici che forniscono servizi primari per il cittadino quali la sicurezza alimentare;

tra i settori individuati dall'articolo 3 del decreto del Presidente del Consiglio dei ministri n. 131 del 2020 in via prioritaria nel Perimetro, non è incluso il settore agroalimentare e pertanto le relative banche dati e informazioni non risultano essere oggetto delle tutele previste dal perimetro di sicurezza entro cui gli operatori del settore possano operare sottraendole alle diverse forme in cui si può manifestare la minaccia cibernetica o gli incidenti informatici, garantendo strumenti per aumentarne la tutela e la capacità di resilienza;

quanto sopra riportato evidenzia la necessità di intervenire a livello normativo ai fini di definire un quadro di riferimento aggiornato e congruente con le disposizioni in vigore e con quelle in fase di recepimento per sviluppare una capacità nazionale di prevenzione, monitoraggio, rilevamento, analisi e risposta per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi cibernetici a reti informatiche, banche dati e *cloud* dei servizi di pubblica utilità quali quelli del settore agroalimentare,

impegna il Governo

ad adottare tutte le iniziative necessarie volte ad ampliare il perimetro di sicurezza nazionale cibernetica anche rispetto a quei soggetti e settori che, anche rientrando tra i prestatori di servizi essenziali, svolgono la propria attività nel settore primario del sistema produttivo nazionale, con riferimento sia alla filiera produttiva agroalimentare che a quella agroindustriale, chiamandoli agli adempimenti previsti dal decreto-legge del 21 settembre 2019, n. 105 e fornendo loro, nello spirito della promozione e diffusione della cultura della sicurezza dei consumatori, gli strumenti necessari per limitare la vulnerabilità fisica delle proprie reti informatiche anche attraverso un'idonea formazione e addestramento.

9/1717-A/**1**. Paolo Emilio Russo.

La Camera,

premesso che:

dall'Analisi Tecnico Normativa (ATN) redatta dal Governo si rileva che il provvedimento in titolo « si pone l'obiettivo, in coerenza con il programma di Governo, di prevenire minacce alla sicurezza informatica con specifiche procedure volte a rendere più immediato l'intervento dell'Agenzia a fini di prevenzione degli attacchi e delle loro conseguenze e del ripristino rapido delle funzionalità dei sistemi informatici »;

sempre l'ATN illustra le ulteriori finalità: « le disposizioni di cui al Capo I sono finalizzate a conseguire una più elevata capacità di protezione e risposta alle emergenze cibernetiche ». L'attuale conte-

sto geo-politico, infatti, caratterizzato in particolare dai gravi conflitti internazionali in atto, favorisce l'incremento delle minacce informatiche e richiede, pertanto, in modo sempre più incalzante, il raggiungimento di un alto livello di cybersicurezza, attraverso l'attuazione di efficaci misure di gestione dei relativi rischi, nonché la necessità di un'immediata e quanto più completa conoscenza situazionale. La proposta normativa risponde alla necessità che si è venuta a profilare sempre di più nell'ultimo periodo di far emergere in modo più puntuale la minaccia informatica diretta ai soggetti della pubblica amministrazione non ricompresi nel Perimetro di sicurezza nazionale cibernetica;

da ultimo, l'ATN, indica « l'obiettivo di garantire un livello comune elevato di cybersicurezza » come richiesto dall'Unione europea, « al fine di rispondere alle crescenti minacce poste dalla digitalizzazione e rafforzare la sicurezza dei soggetti coinvolti nel processo »: si spiega, infatti, che « la direttiva NIS 2 prevede un ampliamento dell'ambito di applicazione, che obbliga più entità e settori ad adottare misure di sicurezza, includendo, per quanto riguarda il settore pubblico, anche le pubbliche amministrazioni. Le disposizioni del Capo I del presente disegno di legge, dunque, rispondono alla necessità di aumentare la resilienza dei soggetti della pubblica amministrazione attualmente non ricompresi nell'ambito di applicazione del decreto-legge 21 settembre 2019, n. 105, né al momento interessati dalla direttiva NIS, tenuto conto del fatto che potrebbero essere interessati dalla direttiva NIS 2 »;

nulla quaestio, ma, ad avviso dei firmatari, tra il menzionato programma e l'azione di Governo c'è di mezzo l'invarianza finanziaria: l'Italia si colloca all'ultimo posto dei Paesi del G7 per quanto riguarda il rapporto tra le spese per la cybersicurezza e il PIL: Italia 0,12 per cento; Stati Uniti 0,34 per cento; Regno Unito 0,29 per cento; Francia e Germania 0,19 per cento – e tutto ciò mentre gli attacchi cibernetici in Italia, come ben descritto nell'ATN e cosi come in tutti i paesi occidentali, sono in crescita esponenziale e di natura sempre più sofisticata;

c'è da domandarsi come possano essere raggiunti gli obiettivi e perseguite tutte le finalità sopra indicate in assenza di costi e, dunque, di risorse per l'Agenzia e le amministrazioni e gli enti che « entrano » quali nuovi soggetti chiamati a rafforzare la loro capacità di resilienza, adeguamento e risposta alla minaccia informatica e cibernetica; il rischio è, dunque, quello di inattuazione o di una attuazione solo formale delle misure di cui al provvedimento in titolo;

in proposito, ai firmatari preme segnalare:

a) i requisiti del referente per la cybersicurezza da nominare in tutte le amministrazioni pubbliche e negli enti coinvolti, requisiti completamente assenti nel testo originario del Governo e tuttora generici e indeterminati, nonostante l'emendamento approvato nel corso dell'esame in sede referente: ciò appare in aperto e netto contrasto con la richiamata volontà, riferita anche nell'ATN, di anticipare il recepimento della direttiva NIS2 con il presente provvedimento, in quanto la direttiva richiede espressamente la definizione e la certificazione delle qualifiche e dei requisiti dei referenti cyber;

in proposito, si rammenta che con un nostro emendamento avevamo proposto, oltre al possesso delle competenze previste per il Responsabile della transizione digitale, che per il referente cyber fossero richieste specifiche competenze in materia di strategie e tecnologie di sicurezza informatica e cibernetica e che le Linee giuda dell'Agenzia definissero percorsi di formazione per i referenti cyber e le modalità per il loro aggiornamento professionale continuo, al fine di rafforzare la capacità di resilienza e risposta delle pubbliche amministrazioni alle minacce e ai rischi informatici e alla loro continua evoluzione, in linea con gli obiettivi della direttiva NIS2;

b) l'assenza di reclutamento di personale tecnico altamente specializzato che rafforzi le strutture operative dell'A-

genzia e, al contempo, di un numero congruo – e delle relative risorse finanziarie – di unità di personale altrettanto specializzato di supporto ai referenti per la cybersicurezza delle amministrazioni e degli enti;

c) è lecito dubitare che la dotazione di personale di cui al reclutamento disposto, per la sola Agenzia, dall'articolo 8 del recente decreto-legge cosiddetto « PNRR 4 » in proposito, anche in questa sede, i firmatari stigmatizzano, oltre alle numerose deroghe, i profili critici di legittimità, del comma 13 del predetto articolo 8, le cui procedure risultano in contrasto con l'ordinamento giuridico e il dettato costituzionale, in quanto escludono la partecipazione di candidati esterni – sia sufficiente a soddisfare « la più elevata capacità di protezione e risposta alle emergenze cibernetiche », in particolare a fronte del contesto geopolitico e dei conflitti in atto, che richiedono « il raggiungimento di un alto livello di cybersicurezza, attraverso l'attuazione di efficaci misure di gestione dei relativi rischi, nonché la necessità di un'immediata e quanto più completa conoscenza situazionale »;

si esprime soddisfazione per l'espunzione dal testo del provvedimento dell'articolo che recava disposizioni in tema di intelligenza artificiale, tuttavia, si manifestano forti perplessità in ordine all'articolo che lo ha sostituito (nel testo approdato in Aula, l'articolo 10), il quale attribuisce all'Agenzia per la cybersicurezza – agenzia sotto controllo governativo – una serie di funzioni tra le quali la promozione dell'utilizzo della crittografia come strumento di cybersicurezza, pretermettendo completamente ogni considerazione sui necessari strumenti di tutela della *privacy*; si segnala, altresì, che le tecniche di crittografia richiedono tecnologie specifiche che attualmente non risultano essere nella disponibilità delle amministrazioni pubbliche e, dunque, anche in questo caso, alle intenzioni non fanno seguito le azioni concrete alle nuove disposizioni non fanno seguito adeguate risorse economiche e tecnologiche;

l'inadeguatezza delle risorse finanziarie e, conseguentemente, anche della tecnologia pone a rischio il raggiungimento degli obiettivi fissati dal provvedimento, l'espletamento delle strategiche funzioni che l'Agenzia assomma nonché, in particolare, la capacità di adeguamento e resilienza richiesta alle pubbliche amministrazioni e agli enti,

impegna il Governo

ferme restando le prerogative parlamentari, a valutare gli effetti applicativi delle disposizioni di cui alla premessa e, in occasione dell'adozione di provvedimenti successivi, a dotare il provvedimento di risorse finanziarie congrue e adeguate alla sua effettiva implementazione e attuazione.

9/1717-A/**2**. Alfonso Colucci, Alifano, Auriemma, Penza.

La Camera,

premesso che:

si esprime soddisfazione per l'espunzione, votata in sede referente, dell'articolo del provvedimento che conferiva all'Agenzia, in ragione del suo ruolo di Autorità nazionale per la cybersicurezza, la promozione e lo sviluppo di ogni iniziativa, anche di partenariato pubblico-privato, concernente le funzioni in materia di intelligenza artificiale quale risorsa utile al rafforzamento della cybersicurezza nazionale;

il 13 marzo 2024 il Parlamento europeo ha approvato in via definitiva il Regolamento europeo sull'intelligenza artificiale, esso reca un quadro normativo armonizzato, sicuro e rispettoso dei diritti fondamentali per l'utilizzo e lo sviluppo dell'intelligenza artificiale nell'Unione europea;

in proposito, preme ai firmatari rammentare che in ordine alla struttura di *governance*, il Regolamento prevede l'istituzione di un Comitato europeo per l'intelligenza artificiale, composto da un rappresentante per Stato membro e dal Garante europeo per la protezione dei dati in veste di osservatore, e da parte di ciascuno Stato membro, l'istituzione di autorità na-

zionali con il compilo di garantire l'applicazione e l'attuazione del Regolamento, composte da esperti del settore tecnologico e di calcolo dei dati di IA, dei diritti fondamentali e delle norme giuridiche, nonché dei rischi per la salute e la sicurezza,

impegna il Governo

ferme restando le prerogative parlamentari, in occasione dell'adozione di successivi provvedimenti in tema di intelligenza artificiale, a scongiurare l'ipotesi che, per il nostro Paese, possa configurarsi l'istituzione di un organismo posto sotto il controllo governativo.

9/1717-A/**3**. Auriemma, Alfonso Colucci, Alifano, Penza.

La Camera,

premesso che:

dalla relazione illustrativa e dall'Analisi Tecnico Normativa (ATN) redatte dal Governo si rilevano obiettivi e finalità del provvedimento in titolo « in coerenza con il programma di Governo », tra i quali, in ordine alle disposizioni di cui al Capo I, il conseguimento di « una più elevata capacità di protezione e risposta alle emergenza cibernetiche. L'attuale contesto geo-politico, infatti, caratterizzano in particolare dai gravi conflitti internazionale in alto, favorisce l'incremento delle minacce informatiche e richiede, pertanto, in modo sempre più incalzante, il raggiungimento di un alto livello di cybersicurezza, attraverso l'attuazione di efficaci misure di gestione dei relativi rischi, nonché la necessità di un'immediata e quanto più completa conoscenza situazionale. La proposta normativa risponde alla necessità che si è venuta a profilare sempre di più nell'ultimo periodo di far emergere in modo più puntuale la minaccia informatica diretta ai soggetti della pubblica amministrazione non ricompresi nel Perimetro di sicurezza nazionale cibernetica »;

anticipando, dunque, alcune delle misure della direttiva europea cosiddetta NIS2, che obbliga più entità e settori ad adottare misure di sicurezza e di capacità di risposta alla minaccia cibernetica, il provvedimento include, per quanto riguarda il settore pubblico, anche le pubbliche amministrazioni, gli enti locali, le loro società *in house* tra i soggetti coinvolti dalle nuove misure;

in proposito, preme segnalare aspetti del provvedimento originario del tutto confliggenti con i buoni intendimenti degli obiettivi e delle finalità illustrate dal Governo, irrisolti anche dopo l'esame in sede referente;

è irragionevole aver optato, per il referente della cybersicurezza, per una posizione indeterminata, priva di specifici requisiti e qualifiche, pur rivestendo un ruolo delicato e di grande responsabilità, a differenza di quanto disposto per il Responsabile per la transizione digitale o per il Responsabile della protezione dati;

è irragionevole, l'assenza della previsione – né aver voluto accogliere in tal senso le proposte dell'opposizione – di corsi di formazione iniziali e di attività formative periodiche per i referenti della cybersicurezza, anche al fine di adeguare consapevolezza e competenze all'evoluzione dei rischi e della tecnologia;

pur apprezzando l'accoglimento della proposta avanzata dai sottoscrittori del presente atto – che impegnava l'Agenzia per la cybersicurezza ad individuare modalità e processi di coordinamento e di mutua collaborazione, anche di livello regionale, tra tutte le amministrazioni coinvolte dal provvedimento e tra i referenti per la cybersicurezza al fine di facilitare la resilienza delle amministrazioni pubbliche – la riformulazione, che muta l'impegno in mera facoltà, ne snatura, ovviamente, l'impatto e il senso;

si coglie, dunque, assenza di formazione, di strumenti di cooperazione, di ruoli in organico per i referenti della cybersicurezza, delle strutture che dovranno assisterli nonché, a differenza di quanto fu previsto, nell'ambito della cultura digitale e a favore dell'alfabetizzazione digitale, l'assenza di iniziative volte a favorire e diffon-

dere la cultura della sicurezza informatica nelle scuole e tra i cittadini, a fronte del massiccio utilizzo della tecnologia, dell'incremento del *phishing* e delle truffe informatiche,

impegna il Governo:

ferme restando le prerogative parlamentari, ad adottare:

ogni misura utile, anche legislativa, affinché, l'Agenzia per la cybersicurezza nazionale si impegni ad individuare modalità di coordinamento con le amministrazioni nonché tra i referenti per la cybersicurezza al fine di facilitare la collaborazione e aumentare le capacità di resilienza, anche prevedendo scambi e collaborazioni con le analoghe istituzioni europee;

ad adottare misure, anche legislative, volte a prevedere corsi di formazione iniziali e di attività formative periodiche per i referenti del cybersicurezza, al fine di adeguare consapevolezza e competenze all'evoluzione dei rischi e della tecnologia;

iniziative, anche legislative, che favoriscano un utilizzo consapevole dei rischi dell'uso della tecnologia informatica da parte dei minori, anche attraverso corsi di formazione nelle scuole volti alla diffusione della sicurezza informatica, al pari di quanto previsto per cultura e l'alfabetizzazione digitale.

9/1717-A/**4**. Alifano, Alfonso Colucci, Auriemma, Penza.

La Camera,

impegna il Governo:

ferme restando le prerogative parlamentari, a valutare l'opportunità di adottare, compatibilmente con i vincoli di finanza pubblica:

ogni misura utile, anche legislativa, affinché, l'Agenzia per la cybersicurezza nazionale si impegni ad individuare modalità di coordinamento con le amministrazioni nonché tra i referenti per la cybersicurezza al fine di facilitare la collaborazione e aumentare le capacità di resilienza, anche prevedendo scambi e collaborazioni con le analoghe istituzioni europee;

ad adottare misure, anche legislative, volte a prevedere corsi di formazione iniziali e di attività formative periodiche per i referenti del cybersicurezza, al fine di adeguare consapevolezza e competenze all'evoluzione dei rischi e della tecnologia;

iniziative, anche legislative, che favoriscano un utilizzo consapevole dei rischi dell'uso della tecnologia informatica da parte dei minori, anche attraverso corsi di formazione nelle scuole volti alla diffusione della sicurezza informatica, al pari di quanto previsto per cultura e l'alfabetizzazione digitale.

9/1717-A/**4**. *(Testo modificato nel corso della seduta)* Alifano, Alfonso Colucci, Auriemma, Penza.

La Camera,

premesso che:

dalla relazione illustrativa e dall'Analisi Tecnico Normativa (ATN) redatte dal Governo si rilevano obiettivi e finalità del provvedimento in titolo « in coerenza con il programma di Governo », tra i quali, in ordine alle disposizioni di cui al Capo I la prevenzione di « minacce alla sicurezza informatica con specifiche procedure volte a rendere più immediato l'intervento dell'Agenzia a fini di prevenzione degli attacchi e delle loro conseguenze e del ripristino rapido delle funzionalità dei sistemi informatici, il conseguimento di una più elevata capacità di proiezione e risposta alle emergenze cibernetiche. L'attuale contesto geopolitico, infatti, caratterizzato in particolare dai gravi conflitti internazionale in alto, favorisce l'incremento delle minacce informatiche e richiede, pertanto, in modo sempre più incalzante, il raggiungimento di un alto livello di cybersicurezza. attraverso l'attuazione di efficaci misure di gestione dei relativi rischi, nonché la necessità di un'immediata e quanto più completa conoscenza situazionale. »;

buoni intendimenti che paiono confliggere con diverse clamorose lacune del

provvedimento, già menzionate in sede referente e che qui si ribadiscono – l'assenza di congrue risorse finanziarie che pone in rischio l'attuazione stessa del provvedimento, la sciatteria nella configurazione del referente per la cybersicurezza privo di un ruolo in organico e di una struttura a sé stante nonché privo di requisiti specifici e determinati, l'assenza di coordinamento tra le istituzioni coinvolte nella risposta alla minaccia cibernetica, in sostanza il rischio di abbandono a se stesse delle amministrazioni locali;

sul tema, preme ai firmatari segnalare la necessità di una maggiore acquisizione della consapevolezza dei rischi cibernetici, la carenza di investimenti pubblici nel settore della cybersicurezza e la carenza di figure professionali adatte e specializzate nella sua gestione, questione che appare paradossale a fronte della crescita e dell'evoluzione sempre più numerosa e sofisticata delle minacce e dei rischi,

impegna il Governo

ferme restando le prerogative parlamentari, ad adottare ogni iniziativa utile, anche legislativa, al fine di adottare un piano di investimenti pubblici in ricerca e sviluppo nel settore della sicurezza informatica nonché di incrementare gli indirizzi accademici e professionali specifici per la formazione di figure nell'ambito delle strategie e tecnologie nonché della sicurezza informatica e cibernetica.

9/1717-A/**5**. Penza, Alfonso Colucci, Alifano, Auriemma.

La Camera,

impegna il Governo

ferme restando le prerogative parlamentari, a valutare l'opportunità di adottare, compatibilmente con i vincoli di finanza pubblica, ogni iniziativa utile, anche legislativa, al fine di adottare un piano di investimenti pubblici in ricerca e sviluppo nel settore della sicurezza informatica nonché di incrementare gli indirizzi accademici e professionali specifici per la formazione di figure nell'ambito delle strategie e tecnologie nonché della sicurezza informatica e cibernetica.

9/1717-A/**5**. *(Testo modificato nel corso della seduta)* Penza, Alfonso Colucci, Alifano, Auriemma.

La Camera,

premesso che:

il provvedimento mira a rafforzare la sicurezza nazionale, a favore delle pubbliche amministrazioni, delle imprese e dei cittadini, anche considerato il rilevante sviluppo di tecnologie potenzialmente aggressive;

esso è volto ad assicurare una più elevata capacità di protezione e risposta a fronte di emergenze cibernetiche, alla luce dell'attuale contesto geo-politico;

in particolare, l'articolo 14, intervenendo sul decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991. n. 203, nella prospettiva del potenziamento degli strumenti investigativi, estende la disciplina delle intercettazioni prevista per i fatti di criminalità organizzata anche ai reati informatici, rimessi al coordinamento del procuratore nazionale antimafia c antiterrorismo;

segnatamente, ai sensi del nuovo comma 3-*bis* introdotto dal citato articolo 14, la disciplina derogatoria in materia di intercettazioni nell'ambito di procedimenti per delitti di criminalità organizzata si applica anche quando si procede in relazione a uno dei gravi delitti informatici (tentati o consumati) rimessi ai sensi dell'articolo 371-*bis*, comma 4-*bis* del Codice di procedura penale al coordinamento del procuratore nazionale antimafia e antiterrorismo:

è fondamentale garantire la piena operatività dello strumento delle intercettazioni anche ai reati cosiddetti « spia », ovvero quelli di corruzione. Invero, è notorio come la corruzione costituisca ormai una delle principali porte di ingresso della criminalità organizzata, ed in particolare,

di quella di stampo mafioso, interessata sempre di più ad insinuarsi nella gestione delle risorse pubbliche e nella economia legale, con un costo per lo Stato di circa 60 miliardi l'anno, determinando, così, perspicue implicazioni economiche e sociali:

il legislatore ha l'obbligo di dotare l'autorità giudiziaria di tutti gli strumenti necessari a cogliere ogni attività in corso o interessi nascosti del malaffare. Nella scorsa legislatura, la legge n. 3 del 2019 cosiddetta Spazzacorrotti ha previsto, tra gli altri, il potenziamento delle intercettazioni per i reati connessi alla corruzione. Inoltre, durante il governo Conte II è stato adottato il decreto-legge n. 161 del 2019, entrato in vigore a settembre 2020 che ha rappresentato una sintesi equilibrata tra l'esigenza di perseguire reati gravi e il diritto alla *privacy* rispetto a fatti non rilevanti;

il *trojan* rappresenta certamente un mezzo imprescindibile per l'emersione dei fenomeni corruttivi e per interrompere sul nascere il *pactum sceleris* tra corrotto e corruttore. L'eliminazione o il depotenziamento dei *trojan* per i reati contro la PA rappresenterebbe un notevole passo indietro rispetto alla normativa attuale, finalmente adeguata agli s*tandard* europei,

impegna il Governo

ad astenersi da qualsivoglia intervento normativo – volto a riformare la disciplina delle intercettazioni in termini più limitativi per l'autorità giudiziaria o comunque peggiorativi, ovvero a depotenziare lo strumento del *trojan*, determinante per l'attività investigativa ed indispensabile per contrastare le più gravi manifestazioni criminose, compresa la corruzione, sulle quali prospera la criminalità organizzata e ancor più la mafia.

9/1717-A/**6**. Cafiero De Raho, D'Orso, Ascari, Giuliano.

La Camera,

premesso che:

il provvedimento mira a rafforzare la sicurezza nazionale, a favore delle pubbliche amministrazioni, delle imprese e dei cittadini, anche considerato il rilevante sviluppo di tecnologie potenzialmente aggressive;

esso è volto ad assicurare una più elevata capacità di protezione e risposta a fronte di emergenze cibernetiche, alla luce dell'attuale contesto geo-politico;

in particolare, il nuovo articolo 22, introdotto in sede referente, reca modifiche all'articolo 7 della legge 12 agosto 1962, n. 1311, in materia di verifiche ispettive negli uffici giudiziari allo scopo di accertare se i servizi procedono secondo le leggi, i regolamenti e le istruzioni vigenti, prevedendo espressamente che nelle ispezioni venga verificato altresì il rispetto delle prescrizioni di sicurezza negli accessi alle banche di dati in uso presso gli uffici giudiziari;

tuttavia, non viene specificato dal legislatore il contenuto delle suddette « prescrizioni di sicurezza », al punto da apparire tale formulazione generica e, pertanto, suscettibile di molteplici interpretazioni;

peraltro nella relazione illustrativa di accompagnamento alla riformulazione dell'emendamento che ha introdotto la suddetta novella, nel descrivere l'oggetto dell'attività ispettiva si fa riferimento non già al rispetto delle « prescrizioni di sicurezza » ma alla verifica della « regolarità degli accessi », locuzione ancora più ampia e generica che ben potrebbe diventare grimaldello per un controllo nel merito delle indagini e quindi per indebite ingerenze da parte degli ispettori ministeriali, con possibile violazione persino del segreto investigativo;

sarebbe, pertanto, opportuno, che il Governo assumesse determinazioni *ad hoc* in merito al precipuo significato da attribuire alle « prescrizioni di sicurezza », in ossequio ai principi costituzionali in materia di determinatezza nelle prescrizioni legislative,

impegna il Governo

a valutare gli effetti applicativi della disposizione citata in premessa, al fine di adot-

tare le opportune iniziative normative volte a subordinare l'entrata in vigore della citata disposizione all'adozione di un regolamento, predisposto dal ministero della giustizia di concerto con il ministero dell'interno, sentita l'Agenzia Nazionale sulla Cybersicurezza e previa trasmissione alle Camere per l'acquisizione del parere delle Commissioni parlamentari competenti, con cui vengano stabilite prescrizioni che garantiscano uniformi *standard* di sicurezza in relazione all'uso dei dispositivi e delle nuove tecnologie in dotazione agli uffici giudiziari, ed in relazione agli accessi alle banche dati in uso agli uffici giudiziari, nonché norme idonee a circoscrivere l'attività ispettiva in modo da evitare possibili indebite ingerenze sul merito delle inchieste e da garantire in modo assoluto il segreto investigativo sulle stesse.

9/1717-A/**7**. D'Orso, Ascari, Cafiero De Raho, Giuliano.

La Camera,

premesso che:

l'articolo 1 del disegno di legge in esame prevede un obbligo di segnalazione di alcune tipologie di incidenti aventi impatto su reti, sistemi informativi e servizi informatici, in carico alle pubbliche amministrazioni centrali; alle regioni e province autonome di Trento e di Bolzano; ai comuni con popolazione superiore a 100.000 abitanti e comunque ai comuni capoluoghi di regione; alle società di trasporto pubblico con bacino di utenza non inferiore a 100.000 abitanti; alle aziende sanitarie locali; alle società *in house* degli enti fin qui richiamati;

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

la materia della sicurezza cibernetica è regolata a livello europeo dalla direttiva (UE) 2016/1148 del 6 luglio 2016 (cosiddetta direttiva NIS – Network and Information Security) che reca misure per 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 interno con il decreto legislativo n. 65 del 18 maggio 2018, che costituisce 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. Tale normativa è stata più recentemente aggiornata dalla direttiva (UE) 2022/2555 del 14 dicembre 2022 (cosiddetta direttiva NIS 2) che ha sostituito il quadro di riferimento in materia, al fine di tener conto di una crescente digitalizzazione del mercato interno e di un panorama in evoluzione delle minacce alla cybersicurezza;

l'articolo 21 della direttiva NIS 2 elenca le misure di gestione dei rischi di cybersicurezza, che comprendono azioni tecniche, operative e organizzative, scelte per essere adeguate e proporzionate al fine di affrontare i rischi per la sicurezza dei sistemi e delle reti informatiche. Tali misure vanno implementate, dai soggetti coinvolti, sia nelle operazioni quotidiane che nella fornitura dei loro servizi affinché sia raggiunto l'obiettivo primario di prevenire, o quantomeno minimizzare l'impatto degli incidenti sia sui destinatari dei servizi offerti, sia su altri servizi correlati. Lo stesso articolo, inoltre, introduce all'approccio « multirischio » che le strategie di gestione dei rischi *cyber* devono adottare il quale mira a garantire che i soggetti siano preparati a fronteggiare un panorama di minacce in evoluzione, proteggendo le infrastrutture critiche e i servizi essenziali;

la previsione dell'adattamento di un approccio « multirischio », come delineato dalla Direttiva recepita, richiede che i soggetti preparino e implementino misure di sicurezza che affrontino un ampio spettro di rischi per la sicurezza delle reti e dei sistemi informativi: oltre alla semplice difesa contro attacchi cibernetici di natura tecnica, è inclusa la prevenzione di rischi derivanti da cause fisiche, errori umani, sia intenzionali che accidentali, processi interni inefficienti e influenze esterne;

divengono quindi elementi fondamentali una valutazione completa dei rischi che sia regolare e approfondita; la considerazione di rischi fisici e ambientali potenzialmente impattanti sulla sicurezza delle informazioni ma anche degli errori umani, della mancanza di formazione sulla sicurezza e della gestione inadeguata dei processi interni quali fattori di rischio significativi; la gestione della catena di approvvigionamento (le vulnerabilità nei prodotti o servizi forniti da terzi possono rappresentare un rischio per la sicurezza); la preparazione di piani dettagliati efficaci di risposta a incidenti di sicurezza di varia natura; lo sviluppo di sistemi e processi che possano adattarsi e resistere a diversi tipi di interruzione al fine di mantenere la continuità operativa nonché la condivisione di informazioni su minacce e vulnerabilità con entità simili e autorità pubbliche per migliorare la capacità collettiva di prevenire e rispondere agli attacchi;

la prevenzione di tali rischi è di dirimente importanza per tutti gli enti pubblici menzionati dal comma 1 del citato articolo 1, pertanto – oltre al non ritenersi sufficiente, al fine della resilienza dell'intero sistema, il solo obbligo di notifica degli incidenti e degli attacchi avvenuti – è fondamentale l'emanazione di linee guida in materia destinate alle pubbliche amministrazioni che chiariscano le modalità con le quali evitare incidenti,

impegna il Governo

ad emanare con la massima urgenza linee guida per i soggetti pubblici di cui all'articolo 1 del disegno di legge in esame, che definiscano le modalità di implementazione delle misure di gestione dei rischi di cybersicurezza indicate all'articolo 21, comma 2, della Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (Direttiva NIS 2), anche al fine di evitare più efficacemente il verificarsi di incidenti informatici.

9/1717-A/**8**. Pastorella.

La Camera,

premesso che:

l'articolo 1 del disegno di legge in esame prevede un obbligo di segnalazione di alcune tipologie di incidenti aventi impatto su reti, sistemi informativi e servizi informatici, in carico alle pubbliche amministrazioni centrali; alle regioni e province autonome di Trento e di Bolzano; ai comuni con popolazione superiore a 100.000 abitanti e comunque ai comuni capoluoghi di regione; alle società di trasporto pubblico con bacino di utenza non inferiore a 100.000 abitanti; alle aziende sanitarie locali; alle società *in house* degli enti fin qui richiamati;

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

la materia della sicurezza cibernetica è regolata a livello europeo dalla direttiva (UE) 2016/1148 del 6 luglio 2016 (cosiddetta direttiva NIS – Network and Information Security) che reca misure per 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 interno con il decreto legislativo n. 65 del 18 maggio 2018, che costituisce 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. Tale normativa è stata più recentemente aggiornata dalla direttiva (UE) 2022/2555 del 14 dicembre 2022 (cosiddetta direttiva NIS 2) che ha sostituito il quadro di riferimento in materia, al fine di tener conto di una crescente digitalizzazione del mercato interno e di un panorama in evoluzione delle minacce alla cybersicurezza;

l'articolo 21 della direttiva NIS 2 elenca le misure di gestione dei rischi di cybersicurezza, che comprendono azioni tecniche, operative e organizzative, scelte per essere adeguate e proporzionate al fine di affrontare i rischi per la sicurezza dei sistemi e delle reti informatiche. Tali misure vanno implementate, dai soggetti coinvolti, sia nelle operazioni quotidiane che nella fornitura dei loro servizi affinché sia raggiunto l'obiettivo primario di prevenire, o quantomeno minimizzare l'impatto degli incidenti sia sui destinatari dei servizi offerti, sia su altri servizi correlati. Lo stesso articolo, inoltre, introduce all'approccio « multirischio » che le strategie di gestione dei rischi *cyber* devono adottare il quale mira a garantire che i soggetti siano preparati a fronteggiare un panorama di minacce in evoluzione, proteggendo le infrastrutture critiche e i servizi essenziali;

la previsione dell'adattamento di un approccio « multirischio », come delineato dalla Direttiva recepita, richiede che i soggetti preparino e implementino misure di sicurezza che affrontino un ampio spettro di rischi per la sicurezza delle reti e dei sistemi informativi: oltre alla semplice difesa contro attacchi cibernetici di natura tecnica, è inclusa la prevenzione di rischi derivanti da cause fisiche, errori umani, sia intenzionali che accidentali, processi interni inefficienti e influenze esterne;

divengono quindi elementi fondamentali una valutazione completa dei rischi che sia regolare e approfondita; la considerazione di rischi fisici e ambientali potenzialmente impattanti sulla sicurezza delle informazioni ma anche degli errori umani, della mancanza di formazione sulla sicurezza e della gestione inadeguata dei processi interni quali fattori di rischio significativi; la gestione della catena di approvvigionamento (le vulnerabilità nei prodotti o servizi forniti da terzi possono rappresentare un rischio per la sicurezza); la preparazione di piani dettagliati efficaci di risposta a incidenti di sicurezza di varia natura; lo sviluppo di sistemi e processi che possano adattarsi e resistere a diversi tipi di interruzione al fine di mantenere la continuità operativa nonché la condivisione di informazioni su minacce e vulnerabilità con entità simili e autorità pubbliche per migliorare la capacità collettiva di prevenire e rispondere agli attacchi,

impegna il Governo

a valutare l'opportunità di emanare con la massima urgenza linee guida per i soggetti pubblici di cui all'articolo 1 del disegno di legge in esame, che definiscano le modalità di implementazione delle misure di gestione dei rischi di cybersicurezza, anche al fine di evitare più efficacemente il verificarsi di incidenti informatici.

9/1717-A/**8**. *(Testo modificato nel corso della seduta)* Pastorella.

La Camera,

premesso che:

l'articolo 1 del disegno di legge in esame prevede l'obbligo di segnalazione di alcune tipologie di incidenti aventi impatto su reti, sistemi informativi e servizi informatici in carico a numerosi soggetti pubblici, tra cui le società di trasporto pubblico con bacino di utenza non inferiore a 100.000 abitanti;

l'obiettivo di tale disposizione è quello di prevedere un più ampio obbligo di notifica di incidenti rilevanti per la cy-

bersicurezza per soggetti ulteriori rispetto a quelli già ricompresi nel perimetro di sicurezza nazionale cibernetica istituito dal decreto-legge 14 giugno 2021, n. 82;

al fine di garantire un'adeguata tutela degli interessi nazionali nel campo della cybersicurezza, così come richiamato dall'articolo 5 del decreto-legge 14 giugno 2021, n. 82, istitutivo dell'Agenzia per la cybersicurezza nazionale (ACN), appare necessario consentire a quest'ultima un maggiore coinvolgimento nella fase preliminare alla notifica degli incidenti rilevanti per la sicurezza informatica, così da consentire un miglioramento del quadro normativo in materia di sicurezza informatica;

inoltre, si osserva che la maggior parte delle agenzie omologhe ad ACN appartenenti ad altri Stati membri dell'Unione europea presentano dipartimenti e servizi dedicati al supporto del settore pubblico e degli enti locali, e che le stesse si stanno preparando con apposite iniziative al fine di accompagnare le nuove entità delle Pubbliche Amministrazioni soggette agli obblighi derivanti dall'implementazione della Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (Direttiva NIS 2),

impegna il Governo

a prevedere la possibilità, per gli enti soggetti all'obbligo di notifica, di avvalersi delle risorse di consulenza e supporto dell'Agenzia per la cybersicurezza nazionale, ivi inclusi corsi di formazione specifica, linee guida e altri strumenti predisposti dalla stessa ACN, necessarie a migliorare i propri standard di sicurezza cibernetica ed implementare le misure di gestione dei rischi di cybersicurezza indicate dall'articolo 21, comma 2, della Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (Direttiva NIS 2).

9/1717-A/**9**. Ruffino, Pastorella.

La Camera,

premesso che:

l'articolo 1 del disegno di legge in esame prevede l'obbligo di segnalazione di alcune tipologie di incidenti aventi impatto su reti, sistemi informativi e servizi informatici in carico a numerosi soggetti pubblici, tra cui le società di trasporto pubblico con bacino di utenza non inferiore a 100.000 abitanti;

l'obiettivo di tale disposizione è quello di prevedere un più ampio obbligo di notifica di incidenti rilevanti per la cybersicurezza per soggetti ulteriori rispetto a quelli già ricompresi nel perimetro di sicurezza nazionale cibernetica istituito dal decreto-legge 14 giugno 2021, n. 82;

al fine di garantire un'adeguata tutela degli interessi nazionali nel campo della cybersicurezza, così come richiamato dall'articolo 5 del decreto-legge 14 giugno 2021, n. 82, istitutivo dell'Agenzia per la cybersicurezza nazionale (ACN), appare necessario consentire a quest'ultima un maggiore coinvolgimento nella fase preliminare alla notifica degli incidenti rilevanti per la sicurezza informatica, così da consentire un miglioramento del quadro normativo in materia di sicurezza informatica;

inoltre, si osserva che la maggior parte delle agenzie omologhe ad ACN appartenenti ad altri Stati membri dell'Unione europea presentano dipartimenti e servizi dedicati al supporto del settore pubblico e degli enti locali, e che le stesse si stanno preparando con apposite iniziative al fine di accompagnare le nuove entità delle Pubbliche Amministrazioni soggette agli obblighi derivanti dall'implementazione della Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (Direttiva NIS 2),

impegna il Governo

a valutare l'opportunità di prevedere un'attività di supporto da parte dell'Agenzia per la cybersicurezza nazionale attraverso l'adozione di linee guida.

9/1717-A/**9**. *(Testo modificato nel corso della seduta)* Ruffino, Pastorella.

La Camera,

premesso che:

l'articolo 1 del disegno di legge in esame prevede l'obbligo di segnalazione di

alcune tipologie di incidenti aventi impatto su reti, sistemi informativi e servizi informatici in carico a numerosi soggetti pubblici, tra cui le società di trasporto pubblico con bacino di utenza non inferiore a 100.000 abitanti;

l'obiettivo di tale disposizione è quello di prevedere un più ampio obbligo di notifica di incidenti rilevanti per la cybersicurezza per soggetti ulteriori rispetto a quelli già ricompresi nel perimetro di sicurezza nazionale cibernetica istituito dal decreto-legge 14 giugno 2021, n. 82;

i processi di digitalizzazione del Paese devono necessariamente essere accompagnati dalla loro messa in sicurezza da possibili attacchi cibernetici. Tuttavia, la componente 2 della missione 1 « Digitalizzazione, innovazione e competitività nel sistema produttivo » del PNRR non prevede un intervento in tal senso e si prevede un investimento di soli 0,62 miliardi di euro in cybersicurezza sui 220 miliardi di euro previsti dal piano, pari allo 0,2 per cento;

secondo il Rapporto « L'ecosistema italiano della sicurezza informatica tra regolazione, competitività e consapevolezza », pubblicato lo scorso 28 febbraio 2023 dall'Osservatorio sulla Cybersicurezza dell'I-Com (Istituto per la competitività), il 48 per cento o delle imprese ritiene poco importante o non rilevante la formazione digitale e solo poco più della metà dei dirigenti riceve una formazione specifica nel campo della cybersicurezza in azienda;

secondo l'indice Desi (*Digital economy and society index*) formulato dalla Commissione europea, l'Italia si trova al diciottesimo posto sui 27 Paesi membri dell'Unione europea per livello di digitalizzazione complessivo, con un punteggio di 49,3 contro una media europea di 52,3. In Italia il livello è particolarmente basso nell'ambito del capitale umano, risultando penultima tra i Paesi membri: in particolare, solo il 46 per cento degli italiani risulta essere in possesso di competenze digitali di base (contro il 54 per cento della media europea) e la quota di laureati in ambito ICT sul totale della popolazione con una laurea risulta essere pari all'1,3 per cento (contro il 3,9 per cento della media europea);

il numero di corsi di formazione in materia di sicurezza cibernetica è in crescita: secondo il già citato Rapporto di I-Com, a gennaio 2023 è stata registrata la presenza di 234 corsi di formazione universitaria (contro i 79 di inizio 2022). I corsi analizzati includono sia insegnamenti singoli all'interno di corsi di laurea generici (« offerta formativa non specializzata »), sia corsi di laurea specifici, insieme a master e dottorati (« offerta formativa specializzata »). Risultano essere attivi 112 insegnamenti singoli all'interno di corsi di laurea magistrale, 56 insegnamenti singoli all'interno delle lauree triennali e 13 corsi singoli all'interno di dottorati di ricerca, a fronte di 4 lauree triennali, 22 lauree magistrali, 7 dottorati e 18 master interamente dedicati alla cybersicurezza,

impegna il Governo:

ad adoperarsi affinché il sistema scolastico e universitario fornisca un'adeguata offerta formativa ed accademica volta a colmare le carenze del Paese riguardanti le competenze, sia di base che avanzate, nel settore della sicurezza cibernetica, anche ampliando la collaborazione tra gli istituti e gli enti della pubblica amministrazione;

ad adottare iniziative volte ad incentivare la formazione in ambito cyber per aumentare il livello di competenze nelle imprese italiane.

9/1717-A/**10**. Grippo, Pastorella.

La Camera,

premesso che:

in sede di discussione del disegno di legge recante: « Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici » è emersa l'improcrastinabilità di prevenire minacce perpetrate con mezzi telematici e informatici e nello stesso tempo realizzare una più forte

tutela della sicurezza cibernetica nazionale;

attualmente la materia è regolata a livello dell'Unione europea dalla direttiva (UE) 2016/1148 del 6 luglio 2016 direttiva NIS – che reca misure per conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, che contribuisce ad incrementare il livello comune di sicurezza nell'Unione europea;

la direttiva è stata recepita con il decreto legislativo del 18 maggio 2018, n. 65, che definisce le misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi dell'Unione europea;

viste le nuove minacce alla cybersicurezza e la divergenza nella sua applicazione tra i vari Stati membri, con un effetto potenzialmente pregiudizievole della sicurezza e del mercato interno, la normativa europea è stata poi aggiornata dalla direttiva (UE) 2022/2555 del 14 dicembre 2022 – direttiva NIS 2 – e la delega per la trasposizione della direttiva nel diritto interno è contenuta nella legge di delegazione europea 2022-2023 – legge 21 febbraio 2024, n. 15 –;

durante il ciclo di audizioni è emerso con chiarezza come il grado di permeabilità delle imprese italiane, di gran lunga superiore alla media mondiale, stia a testimoniare che l'Agenzia nazionale per la cybersicurezza non sta funzionando come dovrebbe e che è necessario un cambio di passo e non passerelle in campagna elettorale;

eppure la costituzione dell'Agenzia per la cybersicurezza nazionale (ANC) e la definizione del perimetro di sicurezza strategica nazionale sono stati dei passaggi molto importanti, ma ora è indispensabile consentire a tale struttura di funzionare nel migliore dei modi, per resistere agli attacchi e per innescare i necessari meccanismi di resilienza, a maggior ragione in conseguenza dei conflitti in atto in Ucraina e in Medio oriente;

alle pubbliche amministrazioni, e a numerosissimi altri soggetti privati, vengono affidati compiti nuovi con conseguente necessità di individuare i relativi referenti, senza che a tali compiti corrispondano gli strumenti economici per formare o per acquisire competenze e personale adeguato per prevenire e reagire agli attacchi. Si arriva al paradosso di scaricare i costi sui soggetti destinatari, anche attraverso il rafforzamento delle sanzioni visto che il provvedimento contiene una clausola di invarianza finanziaria che rischia di stressare eccessivamente il sistema con disposizioni difficili da rispettare;

qui basti solo ricordare l'audizione informale dei rappresentanti di Sogei, i quali hanno sottolineato con chiarezza che in qualsiasi attività compiuta dall'ente sono rintracciabili costi per la tutela della sicurezza cybernetica;

sebbene sul tema della cybersicurezza siano state stanziate diverse risorse dalle leggi di bilancio e dal PNRR 50 milioni di euro previsti alla Missione 1, componente 1 –, queste non sono destinate alle finalità del provvedimento. Comunque a detta dei soggetti auditi, le risorse previste dai bandi dell'Agenzia nazionale per la cybersicurezza sono del tutto insufficienti, anche nell'ipotesi di un loro raddoppio;

si rammenta come l'Italia sia l'ultimo Paese del G7 per quanto riguarda il rapporto tra le spese di cybersicurezza e il PIL, con una percentuale dello 0,12 per cento (a fronte dello 0,19 per cento della Francia e Germania, dello 0,29 per cento del regno Unito e dello 0,34 per cento degli Stati Uniti). Questo nonostante il Documento della strategia nazionale per la cybersicurezza richiami un impegno, confermato dall'Esecutivo, ad investire l'1,2 per cento degli investimenti nazionali lordi sulla cybersicurezza;

purtroppo nel provvedimento manca del tutto una visione generale con riguardo alla tutela della nostra pubblica amministrazione e in modo particolare del settore della sanità, che detiene oltretutto dati significativi sui cittadini italiani;

il digitale è diventato un elemento fondamentale per l'efficienza e la compe-

titività delle imprese, in particolare delle PMI, ma allo stesso tempo ha portato con sé nuovi rischi per la sicurezza dei dati e delle informazioni sensibili. La *cyber security* è diventata una priorità per qualsiasi azienda, grande o piccola che sia, e ignorarla o sottovalutarne l'importanza non è più un'opzione;

sfiora il 46 per cento la quota degli attacchi informatici contro le Pmi da parte dei *cyber* criminali, perché una piccola azienda dispone di mezzi di protezione inferiori, spesso con personale tecnico ridotto se non addirittura assente, e i *cyber* criminali ne sono consapevoli. Il risultato è che le Pmi sono meno preparate in caso di attacco, meno pronte a riconoscere la minaccia e a gestirla tempestivamente, oltre che meno resilienti;

inquietante è l'avviso che hanno lanciato alcune agenzie di intelligenze europee, citate dal *Financial Times*, stando alle fonti citate dal giornale londinese « la Russia ha già iniziato a preparare più attivamente in segreto attentati e atti di sabotaggio per danneggiare le infrastrutture sul territorio europeo, direttamente e indirettamente, senza preoccuparsi delle conseguenze »,

impegna il Governo:

a prevedere, nel prossimo disegno di legge di bilancio, investimenti atti a rispondere ad attacchi di *cyber* criminali che rischiano seriamente di mettere in ginocchio l'economia e la sicurezza del nostro Paese e di violare i dati sensibili dei cittadini;

a prevedere misure idonee a contrastare efficacemente l'ampia diffusione delle truffe online commessi mediante strumenti informatici o telematici idonei ad ostacolare la propria o altrui identificazione, reati che colpiscono prevalentemente soggetti fragili come minorenni, disabili e anziani;

a provvedere ed attuare con urgenza gli investimenti da destinare alla cybersicurezza già previsti dal PNRR alla Missione 1, componente 1;

a prevedere l'assegnazione all'Agenzia per la cybersicurezza nazionale di risorse economiche e unità di personale per far fronte alle nuove funzioni che le sono e saranno attribuite, poiché altrimenti in assenza di investimenti si rischia soltanto di appesantire eccessivamente il sistema con disposizioni difficili da rispettare.

9/1717-A/**11**. Zaratti, Dori, Zanella, Bonelli, Borrelli, Fratoianni, Ghirra, Grimaldi, Piccolotti, Mari.

La Camera,

impegna il Governo:

a valutare l'opportunità, compatibilmente con i vincoli di finanza pubblica, di prevedere, nel prossimo disegno di legge di bilancio, investimenti atti a rispondere ad attacchi di *cyber* criminali che rischiano seriamente di mettere in ginocchio l'economia e la sicurezza del nostro Paese e di violare i dati sensibili dei cittadini;

a proseguire nell'attuazione degli investimenti da destinare alla cybersicurezza già previsti dal PNRR alla Missione 1, componente 1;

a valutare l'opportunità di prevedere, compatibilmente con i vincoli di finanza pubblica, l'assegnazione all'Agenzia per la cybersicurezza nazionale di risorse economiche e unità di personale per far fronte alle nuove funzioni che le sono e le saranno attribuite.

9/1717-A/**11**. *(Testo modificato nel corso della seduta)* Zaratti, Dori, Zanella, Bonelli, Borrelli, Fratoianni, Ghirra, Grimaldi, Piccolotti, Mari.

La Camera,

premesso che:

la rilevante crescita degli attacchi di tipo cibernetico ed il peggioramento dello scenario internazionale ha reso centrale il tema della cybersicurezza al fine di preservare la continuità nell'utilizzo dei *software*,

attraverso processi di prevenzione e di protezione;

nell'ultimo anno, infatti, si è assistito ad un aumento della portata globale degli attacchi i quali si concentrano in particolare nel sottrarre informazioni, monitorare le comunicazioni, o alterare i sistemi di funzionamento;

il Disegno di legge in materia di rafforzamento della cybersicurezza nazionale e dei reati informatici si pone l'obiettivo di rafforzare la normativa volta alla tutela dalle minacce informatiche alla pubblica amministrazione;

in particolare l'articolo 8, al comma 2, istituisce la figura del referente per la cybersicurezza all'interno della pubblica amministrazione;

nello specifico: « il referente per la cybersicurezza, è individuato in ragione di specifiche e comprovate professionalità e competenze. Il referente per la cybersicurezza svolge anche la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale in relazione a quanto previsto dalla presente legge e dalle normative settoriali in materia di cybersicurezza cui è soggetta la medesima amministrazione. A tal fine, il nominativo del referente per la cybersicurezza è comunicato all'Agenzia per la cybersicurezza nazionale »;

l'*European Agency for Cybersecurity* inserisce la formazione e la cultura sulla cybersicurezza ai primi posti nelle linee guida per le aziende al fine di aumentare la protezione cyber a tutti i livelli aziendali;

la maggior parte degli attacchi cibernetici, infatti, avviene a causa di un errore umano causato anche inconsapevolmente, ma dovuto ad una mancata formazione puntuale e aggiornata dei rischi cibernetici che, nel caso del referente per la cybersicurezza, potrebbero compromettere tutto il sistema informatico dell'ente interessato,

impegna il Governo

a valutare l'opportunità, compatibilmente alle previsioni della finanza pubblica, di promuovere interventi mirati alla formazione specialistica dei referenti della cybersicurezza.

9/1717-A/**12**. Alessandro Colucci.

La Camera,

premesso che:

in sede di discussione del disegno di legge recante: « Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici » è emersa l'improcrastinabilità di prevenire minacce perpetrate con mezzi telematici e informatici e nello stesso tempo realizzare una più forte tutela della sicurezza cibernetica nazionale;

attualmente la materia è regolata a livello dell'Unione europea dalla direttiva (UE) 2016/1148 del 6 luglio 2016 – direttiva NIS – che reca misure per conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, che contribuisce ad incrementare il livello comune di sicurezza nell'Unione europea;

la direttiva è stata recepita con il decreto legislativo del 18 maggio 2018, n. 65, che definisce le misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi dell'Unione europea;

viste le nuove minacce alla cybersicurezza e la divergenza nella sua applicazione tra i vari Stati membri, con un effetto potenzialmente pregiudizievole della sicurezza e del mercato interno, la normativa europea è stata poi aggiornata dalla direttiva (UE) 2022/2555 del 14 dicembre 2022 – direttiva NIS 2 – e la delega per la trasposizione della direttiva nel diritto interno è contenuta nella legge di delegazione europea 2022-2023 – legge 21 febbraio 2024, n. 15 –;

durante il ciclo di audizioni è emerso con chiarezza come il grado di permeabilità delle imprese italiane, di gran lunga superiore alla media mondiale, stia a testimoniare che l'Agenzia nazionale per la

cybersicurezza non sta funzionando come dovrebbe e che è necessario un cambio di passo e non passerelle in campagna elettorale;

eppure la costituzione dell'Agenzia per la cybersicurezza nazionale (ACN) e la definizione del perimetro di sicurezza strategica nazionale sono stati dei passaggi mollo importanti, ma ora è indispensabile consentire a tale struttura di funzionare nel migliore dei modi, per resistere agli attacchi e per innescare i necessari meccanismi di resilienza, a maggior ragione in conseguenza dei conflitti in atto in Ucraina e in Medio Oriente;

qui basti solo ricordare l'audizione informale dei rappresentanti di Sogei, i quali hanno sottolineato con chiarezza che in qualsiasi attività compiuta dall'ente sono rintracciabili costi per la tutela della sicurezza cybernetica;

sebbene sul tema della cybersicurezza siano state stanziate diverse risorse dalle leggi di bilancio e dal PNRR – 50 milioni di euro previsti alla Missione 1, componente 1 –, queste non sono destinate alle finalità del provvedimento. Comunque a detta dei soggetti auditi, le risorse previste dai bandi dell'Agenzia nazionale per la cybersicurezza sono del tutto insufficienti, anche nell'ipotesi di un loro raddoppio;

si rammenta come l'Italia sia l'ultimo Paese del G7 per quanto riguarda il rapporto tra le spese di cybersicurezza e il PIL, con una percentuale dello 0,12 per cento (a fronte delle 0,19 per cento della Francia e Germania, dello 0,29 per cento del Regno Unito e dello 0,34 per cento degli Stati Uniti). Questo nonostante il Documento della strategia nazionale per la cybersicurezza richiami un impegno, confermato dall'Esecutivo, ad investire l'1,2 per cento degli investimenti nazionali lordi sulla cybersicurezza;

da quando è operativa, nel gennaio 2022, l'Agenzia per la cybersicurezza nazionale (ACN) si è occupata di 58 attacchi informatici a strutture sanitarie pubbliche, con un impatto critico nella maggior parte dei casi;

che il settore sanitario sia stato il più colpito dal *cybercrime* nel 2022, a confermarlo è stato anche il rapporto *Clusit* 2023 (l'Associazione Italiana per la Sicurezza Informatica): nel mondo, gli attacchi sferrati alla sanità sono stati il 17 per cento sul totale, da gennaio a marzo 2023, contro il 12 per cento del 2022. In particolare, in Italia, gli attacchi a strutture medico-ospedaliere sono triplicate negli ultimi quattro anni;

in un settore come quello della sanità, gli effetti dei crimini informatici non si limitano a risvolti negativi in termini economici o di tutela della *privacy* ma impattano direttamente sulla salute delle comunità e dei privati cittadini. Basti pensare all'attacco *ransomware* che ha colpito le strutture ospedaliere statunitensi della *Prospect Medical Holdings* lo scorso agosto, costringendo a bloccare per qualche giorno visite, operazioni chirurgiche ed approfondimenti diagnostici, causando enormi disagi e ritardi potenzialmente dannosi per la salute dei pazienti;

inquietante è l'avviso che hanno lanciato alcune agenzie di *intelligence* europee, citate dal *Financial Times,* stando alle fonti citate dal giornale londinese la Russia ha già iniziato a preparare più attivamente in segreto attentati e atti di sabotaggio per danneggiare le infrastrutture sul territorio europeo, direttamente e indirettamente, senza preoccuparsi delle conseguenze,

impegna il Governo:

a prevedere l'assegnazione all'Agenzia per la cybersicurezza nazionale di risorse economiche e unità di personale per far fronte alle nuove funzioni che le sono e saranno attribuite, poiché altrimenti in assenza di questi minimi investimenti si rischia soltanto di stressare eccessivamente il sistema con disposizioni difficili da rispettare;

a stanziare risorse economiche adeguate affinché anche il nostro Paese si allinei ai Paesi dell'Unione europea del G7 per quanto riguarda il rapporto tra le spese di cybersicurezza e il PIL, e a tutelare in

maniera particolare il Sistema Sanitario Nazione che è particolarmente vulnerabile.

9/1717-A/**13**. Zanella, Zaratti, Dori, Bonelli, Borrelli, Fratoianni, Ghirra, Grimaldi, Piccolotti, Mari.

La Camera,

premesso che:

in sede di discussione del disegno di legge recante: « Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici » è emersa l'improcrastinabilità di prevenire minacce perpetrate con mezzi telematici e informatici e nello stesso tempo realizzare una più forte tutela della sicurezza cibernetica nazionale;

attualmente la materia è regolata a livello dell'Unione europea dalla direttiva (UE) 2016/1148 del 6 luglio 2016 – direttiva NIS – che reca misure per conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, che contribuisce ad incrementare il livello comune di sicurezza nell'Unione europea;

la direttiva è stata recepita con il decreto legislativo del 18 maggio 2018, n. 65, che definisce le misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi dell'Unione europea;

viste le nuove minacce alla cybersicurezza e la divergenza nella sua applicazione tra i vari Stati membri, con un effetto potenzialmente pregiudizievole della sicurezza e del mercato interno, la normativa europea è stata poi aggiornata dalla direttiva (UE) 2022/2555 del 14 dicembre 2022 – direttiva NIS 2 – e la delega per la trasposizione della direttiva nel diritto interno è contenuta nella legge di delegazione europea 2022-2023 – legge 21 febbraio 2024, n. 15 –;

eppure la costituzione dell'Agenzia per la cybersicurezza nazionale (ACN) e la definizione del perimetro di sicurezza strategica nazionale sono stati dei passaggi mollo importanti, ma ora è indispensabile consentire a tale struttura di funzionare nel migliore dei modi, per resistere agli attacchi e per innescare i necessari meccanismi di resilienza, a maggior ragione in conseguenza dei conflitti in atto in Ucraina e in Medio Oriente;

qui basti solo ricordare l'audizione informale dei rappresentanti di Sogei, i quali hanno sottolineato con chiarezza che in qualsiasi attività compiuta dall'ente sono rintracciabili costi per la tutela della sicurezza cybernetica;

si rammenta come l'Italia sia l'ultimo Paese del G7 per quanto riguarda il rapporto tra le spese di cybersicurezza e il PIL, con una percentuale dello 0,12 per cento (a fronte delle 0,19 per cento della Francia e Germania, dello 0,29 per cento del Regno Unito e dello 0,34 per cento degli Stati Uniti). Questo nonostante il Documento della strategia nazionale per la cybersicurezza richiami un impegno, confermato dall'Esecutivo, ad investire l'1,2 per cento degli investimenti nazionali lordi sulla cybersicurezza;

da quando è operativa, nel gennaio 2022, l'Agenzia per la cybersicurezza nazionale (ACN) si è occupata di 58 attacchi informatici a strutture sanitarie pubbliche, con un impatto critico nella maggior parte dei casi;

che il settore sanitario sia stato il più colpito dal *cybercrime* nel 2022, a confermarlo è stato anche il rapporto *Clusit* 2023 (l'Associazione Italiana per la Sicurezza Informatica): nel mondo, gli attacchi sferrati alla sanità sono stati il 17 per cento sul totale, da gennaio a marzo 2023, contro il 12 per cento del 2022. In particolare, in Italia, gli attacchi a strutture medico-ospedaliere sono triplicate negli ultimi quattro anni;

in un settore come quello della sanità, gli effetti dei crimini informatici non si limitano a risvolti negativi in termini economici o di tutela della *privacy* ma impattano direttamente sulla salute delle comunità e dei privati cittadini. Basti pensare all'attacco *ransomware* che ha colpito

le strutture ospedaliere statunitensi della *Prospect Medical Holdings* lo scorso agosto, costringendo a bloccare per qualche giorno visite, operazioni chirurgiche ed approfondimenti diagnostici, causando enormi disagi e ritardi potenzialmente dannosi per la salute dei pazienti;

inquietante è l'avviso che hanno lanciato alcune agenzie di *intelligence* europee, citate dal *Financial Times*, stando alle fonti citate dal giornale londinese la Russia ha già iniziato a preparare più attivamente in segreto attentati e atti di sabotaggio per danneggiare le infrastrutture sul territorio europeo, direttamente e indirettamente, senza preoccuparsi delle conseguenze,

impegna il Governo

a valutare l'opportunità, compatibilmente con i vincoli di finanza pubblica, prevedere l'assegnazione all'Agenzia per la cybersicurezza nazionale di risorse economiche e unità di personale per far fronte alle nuove funzioni che le sono e le saranno attribuite.

9/1717-A/**13**. *(Testo modificato nel corso della seduta)* Zanella, Zaratti, Dori, Bonelli, Borrelli, Fratoianni, Ghirra, Grimaldi, Piccolotti, Mari.

La Camera,

premesso che:

il disegno di legge recante: « Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici » ha lo scopo di prevenire minacce perpetrate con mezzi telematici e informatici e nello stesso tempo di realizzare una più forte tutela della sicurezza cibernetica nazionale;

durante il ciclo di audizioni è emerso con chiarezza come il grado di permeabilità del sistema Italia, di gran lunga superiore alla media mondiale, stia a testimoniare che l'Agenzia nazionale per la cybersicurezza non sta funzionando come dovrebbe e che è necessario un cambio di passo e non passerelle in campagna elettorale;

eppure la costituzione dell'Agenzia per la cybersicurezza nazionale (ACN) e la definizione del perimetro di sicurezza strategica nazionale sono stati dei passaggi molto importanti, ma ora è indispensabile consentire a tale struttura di funzionare nel migliore dei modi, per resistere agli attacchi e per innescare i necessari meccanismi di resilienza, a maggior ragione in conseguenza dei conflitti in atto in Ucraina e in Medio Oriente;

si rammenta come l'Italia sia l'ultimo Paese del G7 per quanto riguarda il rapporto tra le spese di cybersicurezza e il PIL, con una percentuale dello 0,12 per cento (a fronte dello 0,19 per cento della Francia e Germania, dello 0,29 per cento del regno Unito e dello 0,34 per cento degli Stati Uniti). Questo nonostante il Documento della strategia nazionale per la cybersicurezza richiami un impegno, confermato dall'Esecutivo, ad investire l'1,2 per cento degli investimenti nazionali lordi sulla cybersicurezza;

purtroppo nel provvedimento manca del tutto una visione generale con riguardo alla tutela della nostra pubblica amministrazione e in modo particolare del settore della sanità, che detiene oltretutto dati significativi sui cittadini italiani;

inquietante è l'avviso che hanno lanciato alcune agenzie di *intelligence* europee, citate dal *Financial Times*, stando alle fonti citate dal giornale londinese la Russia ha già iniziato a preparare più attivamente in segreto attentati e atti di sabotaggio per danneggiare le infrastrutture sul territorio europeo, direttamente e indirettamente, senza preoccuparsi delle conseguenze,

impegna il Governo

a provvedere ad attuare con urgenza gli investimenti da destinare alla cybersicurezza già previsti dal Piano nazionale di ripresa e resilienza alla Missione 1, componente 1 anche in considerazione di possibili attacchi informatici, da parte degli

hacker in vista dello svolgimento delle prossime elezioni per il rinnovo del Parlamento europeo.

9/1717-A/**14**. Ghirra, Grimaldi, Zanella, Dori, Zaratti, Bonelli, Borrelli, Fratoianni, Piccolotti, Mari.

La Camera,

premesso che:

il disegno di legge recante: « Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici » ha lo scopo di prevenire minacce perpetrate con mezzi telematici e informatici e nello stesso tempo di realizzare una più forte tutela della sicurezza cibernetica nazionale;

eppure la costituzione dell'Agenzia per la cybersicurezza nazionale (ACN) e la definizione del perimetro di sicurezza strategica nazionale sono stati dei passaggi molto importanti, ma ora è indispensabile consentire a tale struttura di funzionare nel migliore dei modi, per resistere agli attacchi e per innescare i necessari meccanismi di resilienza, a maggior ragione in conseguenza dei conflitti in atto in Ucraina e in Medio Oriente;

si rammenta come l'Italia sia l'ultimo Paese del G7 per quanto riguarda il rapporto tra le spese di cybersicurezza e il PIL, con una percentuale dello 0,12 per cento (a fronte dello 0,19 per cento della Francia e Germania, dello 0,29 per cento del regno Unito e dello 0,34 per cento degli Stati Uniti). Questo nonostante il Documento della strategia nazionale per la cybersicurezza richiami un impegno, con fermato dall'Esecutivo, ad investire l'1,2 per cento degli investimenti nazionali lordi sulla cybersicurezza;

inquietante è l'avviso che hanno lanciato alcune agenzie di *intelligence* europee, citate dal *Financial Times*, stando alle fonti citate dal giornale londinese la Russia ha già iniziato a preparare più attivamente in segreto attentati e atti di sabotaggio per danneggiare le infrastrutture sul territorio europeo, direttamente e indirettamente, senza preoccuparsi delle conseguenze,

impegna il Governo

a proseguire nell'attuazione degli investimenti da destinare alla cybersicurezza già previsti dal Piano nazionale di ripresa e resilienza alla Missione 1, componente 1 anche in considerazione di possibili attacchi informatici, da parte degli *hacker* in vista dello svolgimento delle prossime elezioni per il rinnovo del Parlamento europeo.

9/1717-A/**14**. *(Testo modificato nel corso della seduta)* Ghirra, Grimaldi, Zanella, Dori, Zaratti, Bonelli, Borrelli, Fratoianni, Piccolotti, Mari.

La Camera,

premesso che:

l'articolo 18 del disegno di legge in esame estende la disciplina delle intercettazioni, prevista per i fatti di criminalità organizzata, ai reati informatici rimessi al coordinamento del procuratore nazionale antimafia e antiterrorismo;

il captatore informatico (cosiddetto « trojan ») è un sistema dissimulato, inoculato da remoto, che invade il terreno della riservatezza penetrando anche nelle sfere più intime e private;

infatti, il captatore informatico è uno strumento itinerante, che si sposta di « ambiente » in « ambiente », potenzialmente in grado di accendere la *webcam*, di attivare il microfono e di captare conversazioni, di leggere qualsiasi dato venga archiviato all'interno del cellulare (dagli indirizzi in rubrica, agli SMS, ai messaggi *WhatsApp*, agli appunti salvati nelle note), di visualizzare le fotografie, di registrare la « tracciabilità » del possessore del cellulare funzionando da GPS, di catturare segretamente tutto ciò che viene digitato nel dispositivo, potendo quindi risalire anche ad eventuali *password* o numeri di carte di credito;

il c.p.p. consente peraltro l'utilizzo del trojan esclusivamente per le « intercettazioni di comunicazioni tra presenti ». È fondamentale, per garantire il rispetto del perimetro assegnato dal legislatore a tale mezzo di ricerca della prova, prevedere un divieto espresso che escluda altri impieghi;

le Sezioni Unite della Cassazione nel 2016, sentenza « Scurato », avevano ammesso l'utilizzo del captatore informatico « limitatamente ai procedimenti relativi a delitti di criminalità organizzata, anche terroristica, intendendosi per tali quelli elencati negli articoli 51 commi 3-*bis* e 3-*quater* c.p.p., nonché quelli comunque facenti capo a un'associazione per delinquere, con esclusione del mero concorso di persone nel reato »;

in particolare, le Sezioni Unite hanno chiarito che « deve escludersi la possibilità di compiere intercettazioni nei luoghi indicati dall'articolo 614 codice penale, con il mezzo indicato in precedenza, al di fuori della disciplina derogatoria per la criminalità organizzata di cui all'articolo 13 decreto-legge n. 152 del 1991, convertito in legge n. 203 del 1991, non potendosi prevedere, all'atto dell'autorizzazione, i luoghi di privata dimora nei quali il dispositivo elettronico verrà introdotto, con conseguente impossibilità di effettuare un adeguato controllo circa l'effettivo rispetto del presupposto, previsto dall'articolo 266, comma 2, codice procedura penale », che in detto luogo « si stia svolgendo l'attività criminosa », « è invece consentita la captazione nei luoghi di privata dimora ex articolo 614 codice penale, pure se non singolarmente individuati e se ivi non si stia svolgendo l'attività criminosa, per i procedimenti relativi a delitti di criminalità organizzata, anche terroristica, secondo la previsione dell'articolo 13 decreto-legge n. 152 del 1991 », « per procedimenti relativi a delitti di criminalità organizzata devono intendersi quelli elencati nell'articolo 51, commi 3-*bis* e 3-*quater*, codice procedura penale nonché quelli comunque facenti capo a un'associazione per delinquere, con esclusione del mero concorso di persone nel reato »;

tale pronuncia ha affrontato il tema dell'impossibilità di prevedere in anticipo i luoghi di privata dimora in cui il dispositivo elettronico possa trovarsi, in ragione dell'assenza, all'epoca della sentenza, di una disciplina del captatore informatico, che successivamente è stata introdotta. Il tema affrontato dalle Sezioni Unite ha riguardato, dunque, l'individuazione della possibilità di impiego nei procedimenti relativi a reati di criminalità organizzata;

un'interpretazione, quella della Cassazione, costituzionalmente orientata, finalizzata ad escludere contrasti con gli articoli 14 e 15 della Costituzione;

il legislatore è successivamente intervenuto modificando l'articolo 266 c.p.p.;

così ha previsto la possibilità non solo di ricorrere al captatore informatico per tutti i reati per i quali è consentita l'intercettazione, ammettendo il trojan nei luoghi di privata dimora ove vi sia il « fondato motivo che ivi si stia svolgendo l'attività criminosa », come per le intercettazioni ambientali, nonché imponendo (fuori dei casi di procedimenti in materia di criminalità organizzata o pubblica amministrazione « qualificata »), l'indicazione dei luoghi e del tempo, anche indirettamente determinati, per l'attivazione del captatore. Il legislatore, poi, ha introdotto una disciplina *ad hoc* per i reati contro la pubblica amministrazione, consentendo per tali delitti un utilizzo del trojan nei luoghi di privata dimora « previa indicazione » da parte del Giudice « delle ragioni che ne giustificano l'utilizzo nei luoghi indicati dall'articolo 614 del codice penale »;

pertanto tre sono oggi i regimi applicativi dello strumento di cui si tratta a seconda che si proceda: *a)* per i reati previsti dall'articolo 51, comma 3-*bis* e 3-*quater*, c.p.p.; *b)* per i reati con pena massima non inferiore a cinque anni contro la pubblica amministrazione commessi da pubblici ufficiali o incaricati di pubblico servizio; *c)* per i reati comuni;

è evidente che l'essersi discostati dalla Sentenza Scurato ha prodotto scelte normative disallineate;

in relazione ai delitti di criminalità organizzata, in considerazione della loro eccezionale gravità e pericolosità, è certamente condivisibile la scelta normativa, coerente con la sentenza Scurato, di una più pregnante limitazione della segretezza delle comunicazioni e della tutela del domicilio;

alla luce di ciò, risulta necessario prevedere una disciplina organica che, da un lato, indichi le gravi forme di criminalità per le quali ammettere l'utilizzo del captatore informatico e, dall'altro, dettagli le condizioni applicative e le modalità operative di utilizzo, con l'obiettivo di bilanciare l'accertamento delle ipotesi delittuose ed i principi costituzionali previsti dagli articoli 14 e 15 della Costituzione,

impegna il Governo

a prevedere l'introduzione, nel primo provvedimento utile, di una disciplina organica del captatore informatico che rifletta il miglior bilanciamento tra le esigenze investigative e i principi di cui agli articoli 14 e 15 della Costituzione.

9/1717-A/**15**. Enrico Costa, Pittalis, Boschi.

La Camera,

premesso che:

in forza di un emendamento approvato, da ultimo, nel corso dell'esame svolto nel presente consesso, sono state introdotte anche disposizioni in materia di personale degli organismi di informazione per la sicurezza e, segnatamente, in tema di incompatibilità;

con riguardo agli incarichi di Direttore generale e di Vice Direttore generale del DIS e di Direttore e di Vice Direttore di AISE o di AISI e agli incarichi dirigenziali di prima fascia di preposizione a strutture organizzative di livello dirigenziale generale il divieto di attività lavorativa o professionale o consulenziale nei tre anni successivi alla cessazione dell'incarico può essere superato dall'autorizzazione esclusiva del Presidente del Consiglio o dell'Autorità delegata ove istituita, avuto riguardo alle esigenze di tutela del patrimonio informativo acquisito nel corso dell'incarico e alla necessità di scongiurare pregiudizio alla sicurezza nazionale;

si rammenta che l'articolo 30, comma 3, della legge 3 agosto 2007, n. 124, assegna al Comitato parlamentare per la sicurezza della Repubblica la verifica, in modo sistematico e continuativo, a che l'attività dell'intero « Sistema » si svolga, oltre che nel rispetto della Costituzione e delle leggi, nell'esclusivo interesse della Repubblica, questione che, ad avviso dei firmatari, appare essere pertinente al tema in parola,

impegna il Governo

ferme restando le prerogative parlamentari, ad adottare ogni iniziativa utile, anche legislativa, affinché, con riguardo alle disposizioni per il personale degli organismi di informazione per la sicurezza indicato in premessa, sia prevista, nella procedura di autorizzazione allo svolgimento di attività o all'assunzione di incarichi in deroga alle misure introdotte in tema di incompatibilità, l'espressione del parere del Comitato parlamentare per la sicurezza della Repubblica

9/1717-A/**16**. Pellegrini, Alfonso Colucci, Alifano, Auriemma, Penza.

La Camera,

premesso che:

in sede di discussione del disegno di legge recante: « Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici » è emersa l'improcrastinabilità di prevenire minacce perpetrate con mezzi telematici e informatici e nello stesso tempo realizzare una più forte tutela della sicurezza cibernetica nazionale;

attualmente la materia è regolata a livello dell'Unione europea dalla direttiva (UE) 2016/1148 del 6 luglio 2016 – direttiva N1S – che reca misure per conseguire un livello elevato di sicurezza della

rete e dei sistemi informativi in ambito nazionale, che contribuisce ad incrementare il livello comune di sicurezza nell'Unione europea;

durante il ciclo di audizioni è emerso con chiarezza come il grado di permeabilità degli attacchi *hacker*, di gran lunga superiore alla media mondiale, stia a testimoniare che l'Agenzia nazionale per la cybersicurezza non sta funzionando come dovrebbe e che è necessario un cambio di passo e non passerelle in campagna elettorale;

alle pubbliche amministrazioni, e a numerosissimi altri soggetti privati, vengono affidati compiti nuovi con conseguente necessità di individuare i relativi referenti, senza che a tali compiti corrispondano gli strumenti economici per formare o per acquisire competenze e personale adeguato per prevenire e reagire agli attacchi. Si arriva al paradosso di scaricare i costi sui soggetti destinatari, anche attraverso il rafforzamento delle sanzioni visto che il provvedimento contiene una clausola di invarianza finanziaria che rischia di stressare eccessivamente il sistema con disposizioni difficili da rispettare;

qui basti solo ricordare l'audizione informale dei rappresentanti di Sogei, i quali hanno sottolineato con chiarezza che in qualsiasi attività compiuta dall'ente sono rintracciabili costi per la tutela della sicurezza cybernetica;

si rammenta come l'Italia sia l'ultimo Paese del G7 per quanto riguarda il rapporto tra le spese di cybersicurezza e il PIL, con una percentuale dello 0,12 per cento (a fronte dello 0,19 per cento della Francia e Germania, dello 0,29 per cento del Regno Unito e dello 0,34 per cento degli Stati Uniti). Questo nonostante il Documento della strategia nazionale per la cybersicurezza richiami un impegno, confermato dall'Esecutivo, ad investire l'1,2 per cento degli investimenti nazionali lordi sulla cybersicurezza;

la *Cybersecurity* è diventata una preoccupazione sempre più rilevante nel mondo moderno. Con l'aumento della digitalizzazione, le minacce informatiche sono diventate più sofisticate e più diffuse. Per questo, è importante che aziende, professionisti, organizzazioni e utenti in generale mettano a punto delle strategie di protezione dati;

il rapporto *Clusit* 2023 sulla sicurezza ICT in Italia ha rivelato che il numero di *Cyber* Attacchi nel nostro paese nel 2022 è aumentato del 168,6 per cento rispetto all'anno precedente. Per questo motivo, il tema della sicurezza informatica è divenuto centrale per molte organizzazioni;

desta preoccupazione il contenuto dell'articolo 22 che nel modificare l'articolo 7 della legge 12 agosto 1962, n. 1311, che attribuisce un nuovo « potere » agli ispettori del Ministero della giustizia, assai invasivo, attribuito a un soggetto amministrativo e non giurisdizionale. La formulazione risulta fumosa e ambigua e potrebbe configurarsi, se non opportunamente circostanziata, come un'ingiustificata ingerenza dell'organo politico sull'attività giudiziaria,

impegna il Governo

a chiarire l'esatto perimetro di intervento che si attribuisce agli ispettori del Ministero della Giustizia grazie alla modifica dell'articolo 7 della legge 12 agosto 1962, n. 1311, operata dall'articolo 22 del provvedimento all'esame dell'aula.

9/1717-A/**17**. Dori, Zaratti, Zanella, Bonelli, Borrelli, Fratoianni, Ghirra, Grimaldi, Piccolotti, Mari.

La Camera,

premesso che:

la Strategia Nazionale di Cybersicurezza 2022-2026 redatta dall'Agenzia per la Cybersicurezza Nazionale (ACN) a pagina 12 indica la necessità di una quota percentuale degli investimenti nazionali lordi su base annua pari all'1,2 per cento per raggiungere il conseguimento dell'au-

tonomia tecnologica in ambito digitale, oltre che l'ulteriore innalzamento dei livelli di cybersicurezza nei sistemi informativi nazionali;

il 24 ottobre 2023 la I Commissione, Affari costituzionali, dava parere favorevole all'emendamento 3.14 che interveniva sul disegno di legge di delegazione europea 2022-2023, stabilendo l'obbligatoria applicazione della direttiva (UE) 2022/2555 per i comuni e per le province secondo princìpi di gradualità, proporzionalità e adeguatezza. Successivamente, il 23 novembre 2023 la XIV Commissione, Politiche dell'Unione europea, approvava il medesimo emendamento;

il 14 dicembre, la V Commissione, Bilancio, esprimendo il parere sugli emendamenti osservava tra l'altro che « l'obbligo di applicare la direttiva (UE) 2022/2555 (...) ai comuni e alle province, previsto dal criterio direttivo di cui all'articolo 3, comma 1, lettera a), nella sua attuale formulazione, appare suscettibile di determinare nuovi o maggiori oneri a carico della finanza pubblica », stabilendo che le parole « prevedendo comunque l'obbligo » fossero sostituite da « anche considerando la possibilità », senza così che vi fosse la possibilità di nuovi o maggiori oneri;

il 30 dicembre 2023, l'Aula della Camera, durante la discussione sulla citata legge di delegazione europea 2022-23 approvava, dopo parere favorevole del Governo, un ordine del giorno (n. 9/1342-A/78), con la quale il Governo prendeva l'impegno di trovare le risorse necessarie « al fine di consentire che le misure di massimo livello di cybersicurezza previste dalla Direttiva "NIS 2" siano garantite anche a tutti i comuni ed alle province del nostro Paese, secondo principi di gradualità, proporzionalità e adeguatezza »;

al contrario, il provvedimento oggi in via di approvazione impone nuovi impegni (nuovi oneri non solo per le amministrazioni centrali ma anche per le regioni, per le città metropolitane, per le province, per i comuni, stabilendo, però, che tutto questo debba essere fatto ad invarianza finanziaria,

impegna il Governo

a mantenere l'impegno preso con l'accoglimento dell'ordine del giorno (n. 9/1342-A/78), reperendo quanto prima le risorse necessarie per attuare le misure indispensabili per la cybersicurezza, o, in caso contrario, a sopprimere il citato passaggio (pagina 12) della Strategia Nazionale di Cybersicurezza 2022-2026 redatta dall'Agenzia per la Cybersicurezza Nazionale (ACN).

9/1717-A/**18.** Casu.

La Camera,

premesso che:

la Strategia Nazionale di Cybersicurezza 2022-2026 redatta dall'Agenzia per la Cybersicurezza Nazionale (ACN) a pagina 12 indica la necessità di una quota percentuale degli investimenti nazionali lordi su base annua pari all'1,2 per cento per raggiungere il conseguimento dell'autonomia tecnologica in ambito digitale, oltre che l'ulteriore innalzamento dei livelli di cybersicurezza nei sistemi informativi nazionali;

il 24 ottobre 2023 la I Commissione, Affari costituzionali, dava parere favorevole all'emendamento 3.14 che interveniva sul disegno di legge di delegazione europea 2022-2023, stabilendo l'obbligatoria applicazione della direttiva (UE) 2022/2555 per i comuni e per le province secondo princìpi di gradualità, proporzionalità e adeguatezza. Successivamente, il 23 novembre 2023 la XIV Commissione, Politiche dell'Unione europea, approvava il medesimo emendamento;

il 14 dicembre, la V Commissione, Bilancio, esprimendo il parere sugli emendamenti osservava tra l'altro che « l'obbligo di applicare la direttiva (UE) 2022/2555 (...) ai comuni e alle province, previsto dal criterio direttivo di cui all'articolo 3, comma 1, lettera a), nella sua

attuale formulazione, appare suscettibile di determinare nuovi o maggiori oneri a carico della finanza pubblica », stabilendo che le parole « prevedendo comunque l'obbligo » fossero sostituite da « anche considerando la possibilità », senza così che vi fosse la possibilità di nuovi o maggiori oneri;

il 30 dicembre 2023, l'Aula della Camera, durante la discussione sulla citata legge di delegazione europea 2022-23 approvava, dopo parere favorevole del Governo, un ordine del giorno (n. 9/1342-A/78), con la quale il Governo prendeva l'impegno di trovare le risorse necessarie « al fine di consentire che le misure di massimo livello di cybersicurezza previste dalla Direttiva "NIS 2" siano garantite anche a tutti i comuni ed alle province del nostro Paese, secondo principi di gradualità, proporzionalità e adeguatezza »;

al contrario, il provvedimento oggi in via di approvazione impone nuovi impegni (nuovi oneri non solo per le amministrazioni centrali ma anche per le regioni, per le città metropolitane, per le province, per i comuni, stabilendo, però, che tutto questo debba essere fatto ad invarianza finanziaria,

impegna il Governo

a mantenere l'impegno preso con l'accoglimento dell'ordine del giorno (n. 9/1342-A/78), reperendo quanto prima le risorse necessarie per attuare le misure indispensabili per la cybersicurezza.

9/1717-A/**18.** *(Testo modificato nel corso della seduta)* Casu.

PAGINA BIANCA

Stabilimenti Tipografici
Carlo Colombo S. p. A.

19ALA0090690