RESOCONTO STENOGRAFICO

291

SEDUTA DI LUNEDÌ 13 MAGGIO 2024

PRESIDENZA DEL PRESIDENTE **LORENZO FONTANA**

INDI

DELLA VICEPRESIDENTE **ANNA ASCANI**

I N D I C E

N.B. Il RESOCONTO SOMMARIO è disponibile on line già nel corso della seduta, alla pagina "Resoconti" del sito della Camera dei deputati. Il Resoconto Sommario è corredato di collegamenti ipertestuali verso il Resoconto Stenografico *(Vedi RS)* ed ai documenti di seduta *(Vedi All. A)*.

I documenti esaminati nel corso della seduta e le comunicazioni all'Assemblea non lette in aula sono pubblicati nell'*Allegato A*.

Gli atti di controllo e di indirizzo presentati e le risposte scritte alle interrogazioni sono pubblicati nell'*Allegato B*.

N.B. FRATELLI D'ITALIA: FDI; PARTITO DEMOCRATICO - ITALIA DEMOCRATICA E PROGRESSISTA: PD-IDP; LEGA - SALVINI PREMIER: LEGA; MOVIMENTO 5 STELLE: M5S; FORZA ITALIA - BERLUSCONI PRESIDENTE - PPE: FI-PPE; AZIONE-POPOLARI EUROPEISTI RIFORMATORI-RENEW EUROPE: AZ-PER-RE; ALLEANZA VERDI E SINISTRA: AVS; ITALIA VIVA-IL CENTRO-RENEW EUROPE: IV-C-RE; NOI MODERATI (NOI CON L'ITALIA, CORAGGIO ITALIA, UDC, ITALIA AL CENTRO)-MAIE: NM(N-C-U-I)-M; MISTO: MISTO; MISTO-MINORANZE LINGUISTICHE: MISTO-MIN.LING.; MISTO-+EUROPA: MISTO-+EUROPA.

RESOCONTO STENOGRAFICO

PRESIDENZA DEL PRESIDENTE LORENZO FONTANA

La seduta comincia alle 16.

PRESIDENTE. La seduta è aperta.

Invito il deputato Segretario a dare lettura del processo verbale della seduta precedente.

ROBERTO GIACHETTI*, Segretario*, legge il processo verbale della seduta del 6 maggio 2024.

PRESIDENTE. Se non vi sono osservazioni, il processo verbale si intende approvato.

(È approvato).

Missioni.

PRESIDENTE. Comunico che, ai sensi dell'articolo 46, comma 2, del Regolamento, i deputati in missione a decorrere dalla seduta odierna sono complessivamente 77, come risulta dall'elenco consultabile presso la Presidenza e che sarà pubblicato nell'*allegato A* al resoconto stenografico della seduta odierna *(Ulteriori comunicazioni all'Assemblea saranno pubblicate nell'allegato A al resoconto della seduta odierna)*.

Discussione del disegno di legge: Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (A.C. 1717-A).

PRESIDENTE. L'ordine del giorno reca la discussione del disegno di legge n. 1717-A: Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.

Avverto che lo schema recante la ripartizione dei tempi è pubblicato nell'*allegato A* al resoconto stenografico della seduta del 10 maggio 2024 *(Vedi l'allegato A della seduta del 10 maggio 2024)*.

(Discussione sulle linee generali - A.C. 1717-A)

PRESIDENTE. Dichiaro aperta la discussione sulle linee generali.

I presidenti dei gruppi parlamentari Partito Democratico-Italia Democratica e Progressista e MoVimento 5 Stelle ne hanno chiesto l'ampliamento.

Le Commissioni I (Affari costituzionali) e II (Giustizia) si intendono autorizzate a riferire oralmente.

Ha facoltà di intervenire il relatore per la I Commissione e presidente della I Commissione, onorevole Nazario Pagano.

NAZARIO PAGANO*, Relatore per la I Commissione.* La ringrazio, Presidente. Onorevoli colleghi, l'Assemblea avvia oggi la discussione del disegno di legge del Governo recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", nel testo licenziato dalle Commissioni riunite I e II. L'esame del disegno di legge in sede referente, presso le Commissioni riunite affari costituzionali e giustizia, ha avuto inizio il 13 marzo scorso ed è proseguito con un ampio ciclo di audizioni,

svoltosi tra marzo e aprile, nel corso del quale sono stati auditi, oltre al procuratore nazionale antimafia e antiterrorismo e al presidente dell'Autorità garante per la protezione dei dati personali, anche il direttore del servizio Polizia postale e telecomunicazioni, il direttore dell'unità di informazione finanziaria per l'Italia della Banca d'Italia, rappresentanti della Società generale di informatica (Sogei), di Leonardo Spa, di TIM-Telsy, di Fastweb e di altre società specializzate in cybersicurezza, rappresentanti di categorie e numerosi esperti di sicurezza informatica. Il ciclo di audizioni si è, infine, concluso - come era giusto che fosse - con l'intervento del direttore generale dell'Agenzia per la cybersicurezza nazionale (ANC), prefetto Frattasi.

Al termine dell'esame preliminare, sono state presentate 171 proposte emendative di iniziativa parlamentare, nonché un articolo aggiuntivo da parte del Governo. L'esame degli emendamenti, avviato nella seduta del 7 maggio, si è concluso con il conferimento del mandato ai relatori lo scorso 8 maggio. A seguito dell'approvazione dell'articolo aggiuntivo del Governo e di alcune ulteriori proposte emendative, il provvedimento, ora all'esame dell'Assemblea, è composto da 23 articoli rispetto agli originari 18, distribuiti in 2 Capi, recanti rispettivamente: "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" (articoli da 1 a 14) e "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" (articoli da 15 a 23).

Prima di procedere all'illustrazione dei contenuti del provvedimento, anche a nome del presidente Maschio, relatore per la II Commissione, rammento che la materia della sicurezza cibernetica è regolata a livello di Unione europea dalla direttiva (UE) 2016/1148 del 6 luglio 2016, la cosiddetta direttiva NIS, 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 dell'Unione europea. La direttiva è stata recepita nell'ordinamento interno con il decreto legislativo 18 maggio 2018, n. 65, 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.

La normativa europea è stata successivamente aggiornata dalla direttiva (UE) 2022/2555 del 14 dicembre 2022, la cosiddetta direttiva NIS 2, al fine di tener conto di una crescente digitalizzazione del mercato interno e di un panorama in evoluzione delle minacce alla cybersicurezza e al fine di eliminare le ampie divergenze tra gli Stati membri con riguardo agli obblighi in materia di sicurezza e segnalazione degli incidenti, nonché in materia di vigilanza ed esecuzione.

La delega per la trasposizione della direttiva nel diritto interno è contenuta nella legge di delegazione europea 2022-2023. Successivamente all'attuazione della direttiva NIS 1, il decreto-legge 21 settembre 2019, n. 105, è stato adottato al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei sistemi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi.

Con il decreto-legge n. 82 del 2021 si è proceduto poi alla definizione dell'architettura nazionale di cybersicurezza e all'istituzione dell'Agenzia per la cybersicurezza nazionale, in attuazione di precisi obiettivi del

Piano nazionale di ripresa e resilienza. La sicurezza cibernetica costituisce, infatti, uno dei principali interventi previsti dal PNRR nell'ambito della trasformazione digitale della pubblica amministrazione e della digitalizzazione del Paese.

Passando a illustrare i contenuti del capo I del disegno di legge, segnalo che l'articolo 1, comma 1, come modificato nel corso dell'esame in sede referente, prevede un obbligo di segnalazione di alcune tipologie di incidenti aventi impatto su reti, sistemi informativi e sistemi informatici in carico a determinati soggetti.

Il comma 2 indica le modalità con le quali effettuare la notifica: una prima segnalazione deve avvenire senza ritardo e, comunque, entro il termine massimo di 24 ore dal momento in cui ne sono venuti a conoscenza; entro 72 ore dal medesimo momento dovrà avvenire la notifica completa di tutti gli elementi informativi disponibili.

Il comma 3, inserito in sede referente, dispone che le disposizioni relative alla segnalazione degli incidenti e le modalità per l'effettuazione della notifica si applichino per alcuni soggetti a decorrere dal centottantesimo giorno dalla data di entrata in vigore del provvedimento.

I commi 5 e 6 indicano le sanzioni per la violazione dell'obbligo di notifica.

L'articolo 2, invece, interviene in materia di mancato o ritardato adeguamento a segnalazioni dell'Agenzia per la cybersicurezza nazionale.

L'articolo 3 interviene sull'articolo 1 del decreto-legge n. 105 del 2019, il cosiddetto decreto Perimetro, inserendo due modifiche al comma 3-*bis*, che ha incrementato gli obblighi di notifica posti in capo ai soggetti inclusi nel perimetro di sicurezza nazionale cibernetica: pubbliche amministrazioni, enti e operatori pubblici e privati che svolgono funzioni istituzionali o essenziali per gli interessi dello Stato, individuati con apposito atto amministrativo adottato dal Presidente del Consiglio dei ministri su proposta del Comitato interministeriale per la cybersicurezza.

L'articolo 4, introdotto in sede referente, prevede che i dati relativi a incidenti informatici sono raccolti, sulla base degli adempimenti di notifica previsti a legislazione vigente, dall'Agenzia per la cybersicurezza nazionale, che ne cura la pubblicità come dati ufficiali di riferimento degli attacchi informatici.

L'articolo 5 prevede la possibilità di far partecipare alle riunioni del nucleo per la cybersicurezza ulteriori soggetti quali i rappresentanti della Direzione nazionale antimafia e antiterrorismo e rappresentanti della Banca d'Italia in relazione a specifiche questioni di particolare rilevanza concernenti i compiti di proposta di iniziative in materia di cybersicurezza del Paese.

Poi, l'articolo 6 reca disposizioni in materia di coordinamento operativo dei servizi di informazione per la sicurezza e l'Agenzia per la cybersicurezza nazionale.

L'articolo 7, introdotto nel corso dell'esame in sede referente, modifica la composizione del Comitato interministeriale per la sicurezza della Repubblica.

L'articolo 8, modificato anch'esso in sede referente, istituisce per le pubbliche amministrazioni indicate nell'articolo 1, comma 1, dove non sia già presente, la struttura preposta all'attività di cybersicurezza. Al contempo, predispone l'istituzione del referente per la cybersicurezza, unico punto di contatto delle amministrazioni coinvolte con l'Agenzia per la cybersicurezza nazionale. Precisa, in tal senso, quali soggetti e quali organi dello Stato siano esclusi dall'applicazione dei nuovi obblighi e per cui permane la disciplina precedente. Infine, introduce una specifica disciplina che regola l'accesso alle banche dati delle pubbliche amministrazioni da parte degli addetti tecnici attraverso specifici sistemi di autenticazione.

L'articolo 9, introdotto anch'esso in sede referente, attribuisce alle strutture preposte all'attività di cybersicurezza nelle PA la funzione di verificare che i programmi e le applicazioni informatiche di comunicazione

elettronica rispettino le linee guida sulla crittografia, nonché quelle sulla conservazione delle *password* adottate dall'Agenzia per la cybersicurezza nazionale e dall'Autorità garante per la protezione dei dati personali e non contengano vulnerabilità.

L'articolo 10, interamente sostituito nel corso dell'esame in sede referente, valorizza l'utilizzo della crittografia quale strumento di difesa cibernetica e istituisce il Centro nazionale di crittografia presso l'Agenzia per la cybersicurezza nazionale. La disposizione istituisce presso l'ACN, l'Agenzia appunto, il Centro nazionale di crittografia, con funzioni di centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato, ossia non coperto dal segreto. Il funzionamento del Centro è disciplinato con provvedimento del direttore generale dell'Agenzia. L'articolo in esame fa salve le competenze dell'Ufficio centrale per la segretezza.

Passiamo all'articolo 11, che definisce tempi e modalità per l'adozione del regolamento che dovrà stabilire 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.

L'articolo 12, introducendo il comma 8-*ter* all'articolo 12 del decreto-legge n. 82 del 2021, stabilisce un divieto, della durata di due anni, di assunzione, anche di incarichi, presso soggetti privati, finalizzata allo svolgimento di mansioni in materia di cybersicurezza per i dipendenti appartenenti al ruolo del personale dell'Agenzia per la cybersicurezza nazionale che abbiano partecipato, nell'interesse o a spese dell'Agenzia stessa, a specifici percorsi formativi di specializzazione.

L'articolo 13 introduce alcuni criteri di cybersicurezza nella disciplina dei contratti pubblici. In dettaglio, il comma 1 prevede l'adozione di un decreto del Presidente del Consiglio dei ministri entro 120 giorni dalla data di entrata in vigore del provvedimento in esame, su proposta dell'Agenzia per la cybersicurezza nazionale e previo parere del Comitato interministeriale per la sicurezza della Repubblica, per individuare, per determinate categorie tecnologiche di beni e servizi, gli elementi essenziali di cybersicurezza da tenere in considerazione in relazione alle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici.

Il comma 2 prevede, nell'ambito dei contratti di approvvigionamento di beni e servizi informatici di cui al comma 1, una serie di obblighi e facoltà in capo alle stazioni appaltanti, incluse le centrali di committenza, in relazione agli elementi essenziali di cybersicurezza individuati dal comma precedente. Tale regolamentazione troverà applicazione per le PA, i gestori dei servizi pubblici e le società a controllo pubblico, ma anche, in base al comma 3, per gli altri soggetti privati rientranti nel perimetro di sicurezza nazionale cibernetica di cui all'articolo 1, comma 2-*bis*, del decreto-legge n. 105 del 2019.

Infine, il capo I si chiude con l'articolo 14, introdotto in sede referente, volto a inserire nell'articolo 16 della legge di delegazione europea 2022-2023 nuovi principi e criteri direttivi specifici a cui il Governo dovrà attenersi nel recepimento della normativa europea in materia di resilienza operativa digitale per il settore finanziario.

Passando a illustrare i contenuti del capo II, rilevo che l'articolo 15 contiene modifiche al codice penale. La lettera *a)*, introdotta in sede referente, interviene sull'articolo 240 del codice penale (confisca) per prevedere, in relazione alla nuova aggravante che le Commissioni hanno inserito in questo provvedimento alla lettera *t)* con riguardo alla truffa aggravata, che si applichi la misura di sicurezza della confisca obbligatoria dei beni e degli strumenti informatici o telematici utilizzati in tutto o in parte per la commissione del reato, nonché dei beni che costituiscono il profitto o il prodotto del reato medesimo, ovvero di somme di denaro, beni o altre utilità di cui il colpevole

ha la disponibilità per un valore corrispondente a tale profitto prodotto, se non è possibile eseguire la confisca diretta del profitto o del prodotto.

La lettera *b)* interviene sull'articolo 615-*ter* del codice penale, cioè accesso abusivo ad un sistema informatico o telematico. La lettera *c)* interviene sull'articolo 615-*quater* del codice penale, cioè detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici. La lettera *d)* abroga l'articolo 615-*quinquies* del codice penale, il cui contenuto è, però, integralmente riprodotto dal nuovo articolo 635-*quater*.1, introdotto dalla lettera *p)*, cui si rinvia. La lettera *e)* interviene sull'articolo 617-*bis* del codice penale (detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti ad intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche). La lettera *f)* interviene sull'articolo 617-*quater* del codice penale (intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche). La lettera *g)* interviene sull'articolo 617-*quinquies* del codice penale (detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti ad intercettare, impedire o interrompere le comunicazioni informatiche o telematiche).

La lettera *h)* interviene sull'articolo 617-*sexies* del codice penale, concernente "Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche".

La lettera *i)* reca una disposizione di coordinamento volta a modificare la rubrica del Capo III-*bis* del Titolo XII del Libro II del codice penale.

La lettera *l)* prevede l'inserimento dell'articolo 623-*quater* del codice penale ("Circostanze attenuanti"), con riguardo ai delitti oggetto di intervento del presente provvedimento, cioè i reati informatici.

La lettera *m)* integra l'articolo 629 del codice penale ("Estorsione"), al fine di punire la fattispecie del delitto di estorsione mediante reati informatici realizzata dalla costrizione di taluno a fare o omettere qualche cosa procurando a sé o a un altro un ingiusto profitto mediante le condotte o la minaccia di compierle di cui ai reati ivi richiamati.

La lettera *n)* interviene sull'articolo 635-*bis* del codice penale ("Danneggiamento di informazioni, dati e programmi informatici").

La lettera *o)* interviene sull'articolo 635-*ter* ("Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità").

La lettera *p)* interviene sull'articolo 635-*quater* ("Danneggiamento di sistemi informatici o telematici"). La lettera *q)* introduce l'articolo 635-*quater*.1 ("Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico").

La lettera *r),* come Roma, novella l'articolo 635-*quinquies* ("Danneggiamento di sistemi informatici o telematici di pubblica utilità"), sostituendo nella rubrica e nel testo le parole "pubblica utilità" con "pubblico interesse" e innalzando la pena della reclusione da 2 a 6 anni. Attualmente la pena prevista, invece, è da 1 a 4.

La lettera *s)* inserisce l'articolo 639-*ter*, "Circostanze attenuanti", per questa tipologia di reati.

In sede referente è stata inserita la lettera *t)* che inserisce nell'articolo 640 ("Truffa") un'ulteriore circostanza aggravante - n. 2-*ter* - nel caso in cui il fatto sia commesso a distanza attraverso strumenti informatici o telematici idonei ad ostacolare la propria o altrui individuazione.

In sede referente è stata altresì inserita la lettera *u)* che interviene sull'articolo 640 -*quater* per rendere applicabili, ove ricorra la nuova circostanza aggravante del reato di truffa testé richiamato, le disposizioni contenute nell'articolo 322-*ter* che stabilisce, in caso di condanna o di applicazione della pena, su

richiesta delle parti, la confisca dei beni che costituiscono il profitto o il prezzo del reato, salvo che appartengano a persona estranea al reato.

L'articolo 16 reca modifiche al codice di procedura penale finalizzate a recepire gli interventi in materia di prevenzione e contrasto dei reati informatici introdotti all'articolo 11. La lettera *a)* interviene sull'articolo 51 del codice di procedura penale ("Uffici del pubblico ministero. Attribuzioni del procuratore della Repubblica distrettuale") e reca il catalogo dei reati informatici attribuiti alla competenza del procuratore distrettuale.

Le lettere *b)* e *c)* estendono ai reati informatici le deroghe relative al regime ordinario di notifica dell'avviso della richiesta di proroga delle indagini preliminari e di fissazione dell'udienza in camera di consiglio da parte del GIP in caso di mancato accoglimento dell'istanza.

L'articolo 17 reca alcune modifiche alle norme sui collaboratori di giustizia, di cui al decreto-legge n. 8 del 1991.

L'articolo 18 estende la disciplina delle intercettazioni prevista per i fatti di criminalità organizzata ai reati informatici rimessi al coordinamento del Procuratore nazionale antimafia e antiterrorismo.

L'articolo 19 interviene sul catalogo dei reati presupposto della responsabilità amministrativa degli enti contemplato dall'articolo 24-*bis* del decreto legislativo n. 231 del 2001.

L'articolo 20 interviene sul procedimento di applicazione delle speciali misure di protezione per i testimoni di giustizia e per gli altri protetti, prevedendo che la commissione centrale debba richiedere il parere del Procuratore nazionale antimafia e antiterrorismo sulla proposta di ammissione alle speciali misure, anche nel caso di gravi delitti informatici.

L'articolo 21 disciplina i rapporti tra l'Agenzia per la cybersicurezza nazionale, il Procuratore nazionale antimafia e antiterrorismo e la Polizia giudiziaria con il pubblico ministero.

Ho quasi concluso, mancano davvero poche righe, Presidente. In sede referente è stato introdotto l'articolo 22, che interviene sulla vigente disciplina in materia di visite ispettive da parte dell'Ispettorato generale presso il Ministero della Giustizia.

L'articolo 23, infine, reca le disposizioni finanziarie, recando la consueta clausola di invarianza degli oneri e disponendo che i proventi delle sanzioni di cui all'articolo 1, comma 5, confluiscano nelle entrate dell'Agenzia per la cybersicurezza nazionale. Presidente, ho concluso la relazione.

PRESIDENTE. Ha facoltà di intervenire la rappresentante del Governo, che si riserva di farlo successivamente.

È iscritto a parlare il deputato Penza. Ne ha facoltà.

PASQUALINO PENZA (M5S). Grazie, Presidente. Onorevoli colleghi, oggi, in discussione generale sul disegno di legge sulla cybersicurezza non possiamo che approfondire il tema facendo un *excursus* sull'era digitale, l'era che oggi vede un grande proliferare, quasi alla pari, se non di più, della rivoluzione industriale. Oggi ci troviamo in un contesto in cui la digitalizzazione, la connettività sono all'ordine del giorno: fanno parte della nostra vita. È inconcepibile andare avanti in un contesto mondiale senza il digitale e pensare che il digitale non abbia avuto nel tempo un impatto anche nel mondo del lavoro, nella vita quotidiana di ognuno di noi. Le sfide che oggi l'era digitale ci pone davanti sono tantissime.

In questo contesto, come abbiamo detto, si inserisce quella che è definita la società digitale, una società che è cresciuta, è cambiata, è diventata un'altra rispetto a quella che abbiamo sempre visto prima degli anni Settanta.

Abbiamo visto crescere a dismisura il mondo del *web*, che è partito da una versione detta 1.0, in cui il *web* era come una grande enciclopedia a cui tutti gli utenti potevano accedere e semplicemente consultare i dati che venivano messi a disposizione dai vari *server*, dai vari siti. Poi, tale contesto si è evoluto

ancora una volta, con il *web* 2.0, che vedeva l'utente finalmente interagire con i servizi offerti dai vari siti Internet. Successivamente, c'è stata un'altra evoluzione: quella del *web* 3.0, che stiamo vedendo emergere, ovvero un'esperienza immersiva, totale dell'utente nel mondo del *web* e del digitale, finanche ad arrivare a un futuro 4.0, con l'affacciarsi dell'intelligenza artificiale.

In questo contesto, è diventato indispensabile cercare qualcosa che potesse dare una sorta di disciplina, una sorta di protezione. Ecco perché, in tutto questo emergere del *web*, non si è potuto non notare i pericoli che potessero celarsi dietro allo stesso. Possiamo immaginare attacchi informatici, ma dove vanno a mirare esattamente? Mirano alla *privacy* dei cittadini, alla vita quotidiana dei cittadini.

Oggi, ognuno di noi è iscritto presso un'anagrafe digitale, ognuno di noi è iscritto al comune, con dati personali, anche con riferimento alla sanità pubblica; i nostri dati bancari sono tutti elementi di una certa delicatezza, che vanno perciò protetti con le giuste misure, con misure che siano sinonimo di resilienza, di miglioramento, misure che servano ad introdurre lo Stato nel contesto digitale. Quindi, lì dove ci sono pericoli, lo Stato deve intervenire per tutelare i propri cittadini, per tutelare i nostri dati.

In questo disegno di legge possiamo accogliere come positivo il fatto che si sia finalmente svolto un esame con i dovuti canoni.

Ci sono state audizioni molto proficue, ci sono state delle discussioni, c'è stata una votazione che ha portato a compimento il proprio scopo, ovvero non c'è stata un'interruzione anticipata, ma siamo riusciti ad arrivare alla fine. Però, non possiamo non evocare alcune carenze, alcune mancanze in questo disegno di legge. Per esempio, la prima mancanza è l'investimento che questo disegno di legge praticamente non prevede in questo contesto, ovvero possiamo provare a pensare che l'Italia, nel rapporto tra PIL e cybersicurezza, ha soltanto lo 0,12 per cento, mentre Paesi come gli Stati Uniti hanno lo 0,34, il Regno Unito lo 0,29, Francia e Germania lo 0,19.

Anche in questo contesto noi ci troviamo, purtroppo, a fare il fanalino di coda. Non si può pensare di affrontare questo scenario senza un investimento di bilancio adeguato. In questo provvedimento manca la costituzione di un quadro coordinato, ovvero con strutture decentrate, modelli di rete che servono anche a proteggere i nostri sistemi informatici, collaborazione con le università, che abbiamo visto assenti in questo provvedimento. Non possiamo non pensare che non vengono definiti i requisiti di professionalità: i referenti per la cybersicurezza che percorsi formativi devono avere, di cosa si occuperanno, saranno ingegneri, saranno informatici? Questo non viene disciplinato, non viene chiarito.

Una cosa importante è anche l'educazione alla cybersicurezza, ma un'educazione che va mirata al cittadino. In questo decreto non viene programmato un *modus* per poter educare il cittadino alla cybersicurezza. Non possiamo pensare di avere una cybersicurezza laddove gli utenti che utilizzano il *web* per interagire con lo Stato e tra di loro non conoscano i principi cardine per poter essere protetti nel mondo del *web*. E, allora, lì vediamo persone che spesso vengono truffate: ricevono un messaggio, magari, che gli viene inviato dal figlio, ma non è un messaggio del figlio; aprono il *link* e in quel momento i loro dati entrano in possesso di estranei.

Se noi accendiamo la TV e guardiamo per un attimo un programma a caso, *Le Iene*, vediamo quante persone possono cadere in questa trappola. Allora, ragionare su un sistema anche di educazione per chi magari oggi non è più giovanissimo, ma ha bisogno di aggiornamenti, potrebbe essere un buon punto, che però non troviamo in questo disegno di legge.

L'approccio sanzionatorio che viene anche previsto in questo contesto lo vediamo quasi inapplicabile. Chi utilizza strumenti informatici per commettere cybercrimini non

ci va con l'etichetta "sono Tizio, sono Caio". Loro adotteranno sicuramente dei sistemi di offuscamento, quindi si rende ancora più difficile l'identificazione del cybercriminale. Allora, noi dovevamo prevedere un sistema anche di studio con le università, investendo in cybersicurezza. La sicurezza si fa investendo, mettendoci soldi. È impossibile fare sicurezza senza soldi, è impossibile. Questo potrebbe essere un primo approccio, ma non è sufficiente; potrebbe essere un inizio, ma dobbiamo capire che in futuro bisogna migliorare, bisogna andare avanti.

Noi abbiamo apprezzato, invece, la nostra proposta di soppressione dell'articolo 7, che prevedeva di affidare all'Agenzia per la cybersicurezza nazionale la vigilanza sull'intelligenza artificiale. Noi lì vediamo un conflitto effettivamente: lo Stato non può avocare a sé un tale controllo perché c'è bisogno di una vera e propria separazione di alcuni compiti.

L'intelligenza artificiale, che noi oggi stiamo vedendo e vediamo sui nostri computer o nelle immagini o nelle foto che spesso troviamo sui nostri telefonini, è una nuova tecnologia che sta avanzando in maniera veramente vertiginosa, e lo fa senza che noi ce ne rendiamo conto. Oggi vediamo una traduzione fatta in tempo reale di un video magari registrato pochi minuti prima, e vediamo il personaggio del video parlare 2 o 3 lingue, quasi come se veramente stesse parlando lui, con lo stesso tono di voce, con la stessa movenza della bocca. Oppure, che ne so, possiamo pensare che l'intelligenza artificiale un domani potrà sostituire l'uomo in molti percorsi lavorativi. È vero: l'uomo, ad oggi, non è sostituibile al 100 per cento, ma non possiamo non tenere in considerazione che molti lavori andranno via via scomparendo perché l'intelligenza artificiale permetterà all'essere umano di andare avanti con meccanismi veramente sofisticati. La differenza noi l'abbiamo notata nel giro di un anno. Proviamo a pensare al grande passo in avanti che ha fatto la tecnologia dagli anni Settanta ad oggi. Man mano, ci muoviamo sempre più veloci e vediamo che l'intelligenza artificiale, fino a un anno e mezzo fa, si limitava semplicemente a scrivere un testo quasi sensato, per poi diventare veramente un qualche cosa in più, andando sulle immagini, sui video.

E non possiamo non pensare come la moneta digitale sia entrata nella nostra vita e come oggi siano presenti i bitcoin oppure altri sistemi informatici di pagamento. Quindi, è importante investire nelle università per studiare queste tecnologie, capire come applicarle nel modo giusto e in modo resiliente; è quella l'importanza, secondo me, dello studiare l'informatica. La *blockchain*: noi dobbiamo immaginare questa tecnologia che non è nata certo oggi, ma che oggi è alla base di molti sistemi informatici e monetari.

Presidente, vedo che in questo decreto c'era molto da fare, si poteva veramente fare tanto, e spero che il Governo faccia tesoro di questa riflessione, perché le sfide che ci aspetteranno da qui ai prossimi anni non saranno semplici. Ma di una cosa sono sicuro: saranno tutte sfide informatiche che ci metteranno a dura prova, metteranno a dura prova i cittadini, metteranno a dura prova il Governo, gli amministratori locali, in un Paese, come l'Italia, che deve necessariamente muoversi in modo veloce per stare al passo con gli altri Paesi. Questa è la vera essenza.

Noi non dobbiamo più essere il fanalino di coda dell'Europa o del mondo intero, noi dobbiamo essere promotori, dobbiamo essere innovatori. L'Italia e gli italiani hanno tutti i requisiti e soprattutto le capacità per non essere da meno, per non essere gli ultimi, per essere protagonisti anche in un settore informatico come quello dell'intelligenza artificiale. Sono fiducioso che nei prossimi anni ci saranno grandi risvolti, però questo Governo deve capire che bisogna investire, bisogna dare indicazioni chiare. C'è bisogno di una normazione che sia veramente mirata a definire determinati caratteri.

Non a caso, prima ho accennato al fatto che non vengono delineate delle figure chiave e non viene stabilito quali requisiti queste figure

debbano avere. Non vengono specificati, ma è importante avere concetti chiari, è importante capire le competenze, è importante capire la formazione, è importante investire anche nella formazione dei cittadini, nelle scuole. È importante far capire cosa vuol dire sicurezza informatica, la protezione della *privacy*, la protezione dei dati sensibili, la differenza tra dati sensibili e dati riservati. Tutta questa materia la troviamo in modo molto scarso in questo disegno di legge, che, se vogliamo, può essere considerato come un inizio, ma non un inizio completo, motivo per il quale noi ci siamo astenuti sul mandato al relatore in Commissione.

Con questo concludo, Presidente, sperando che si possano poi riesaminare determinati aspetti per un miglioramento futuro di questo disegno di legge *(Applausi dei deputati del gruppo MoVimento 5 Stelle)*.

PRESIDENTE. È iscritto a parlare l'onorevole Sbardella. Ne ha facoltà.

LUCA SBARDELLA (FDI). Signor Presidente, onorevoli colleghi, il disegno di legge all'esame dell'Aula, recante disposizioni in materia di reati informatici e di rafforzamento della cybersicurezza nazionale venne approvato dal Consiglio dei ministri lo scorso 25 gennaio. Il Consiglio dei ministri, su proposta del Presidente, Giorgia Meloni, e del Ministro della Giustizia, Nordio, lo ha approvato con l'auspicio di una sollecita calendarizzazione in ordine soprattutto al delicato tema che si propone di regolamentare. Si tratta di questioni strategiche per la sicurezza nazionale in tempi di pace e, a maggior ragione, in periodi in cui i conflitti internazionali e la guerra ibrida messa in atto da diversi gruppi minacciano la sicurezza informatica degli Stati.

L'esame in Commissione è stato molto approfondito e ha ben coinvolto anche le opposizioni, come riconosciuto anche da alcune di esse in sede di votazione del mandato al relatore.

Governo e maggioranza hanno mostrato grande apertura e disponibilità a valutare nel merito anche l'approvazione di significativi emendamenti presentati dai gruppi di minoranza. Che ci possano essere ancora punti da migliorare in futuro è possibile, ma francamente ora è tempo, proprio per la materia oggetto del disegno di legge, di approvare queste norme importanti per un settore strategico come la difesa della cybersicurezza nazionale.

Nel frattempo che il Parlamento discute e approfondisce, anche in questo istante, le diverse strutture interessate dagli attacchi *cyber* lavorano con difficoltà a legislazione vigente con i limiti di normative vecchie e inadeguate per contrastare il crimine. Si tratta di atti criminali con forte rilevanza ed impatto anche di natura economica. Per questo motivo è importante che l'approvazione del provvedimento sia veloce per consentire al Paese di dotarsi al più presto di strumenti che, per quanto le opposizioni possano dirsi non pienamente soddisfatte, sono certamente più adeguati di quelli attuali.

Questo testo interviene, infatti, con modifiche sostanziali e processuali, in relazione ai reati informatici, prevedendo l'innalzamento delle pene, l'ampliamento dei confini del dolo specifico, l'inserimento di aggravanti e il divieto di attenuanti per diversi reati commessi mediante l'utilizzo di apparecchiature informatiche e finalizzati a produrre indebiti vantaggi per chi li commette a danno altrui, ad accedere abusivamente a sistemi informatici o a intercettare e a interrompere comunicazioni informatiche e telematiche. Si propone, inoltre, di rafforzare le funzioni dell'Agenzia per la cybersicurezza nazionale e il suo coordinamento con l'autorità giudiziaria in casi di attacchi informatici con specifiche procedure volte a rendere più immediato l'intervento dell'Agenzia ai fini di prevenzione degli attacchi e delle loro conseguenze e del ripristino rapido delle funzionalità dei sistemi informatici.

Il disegno di legge si propone di assicurare una più elevata capacità di protezione e

risposta a fronte di emergenze cibernetiche. Alla luce dell'attuale contesto geopolitico, si tratta di una questione non più rinviabile e non è un caso che la sicurezza cibernetica costituisca uno dei principali interventi previsti dal PNRR nell'ambito della trasformazione digitale della pubblica amministrazione e della digitalizzazione del Paese. È un obiettivo totalmente condivisibile, anche considerato il rilevante sviluppo di tecnologie potenzialmente aggressive. Per questo si prevede una *governance* centralizzata degli aspetti di sicurezza e nuove disposizioni per la prevenzione e il contrasto dei reati informatici.

Ricordo, inoltre, che, nell'esprimere il parere favorevole, la XIV Commissione ha rilevato come le norme previste dal presente disegno di legge siano ben coerenti con la legge di delegazione europea 2022-2023, che ha delegato il Governo a dare attuazione alla nuova direttiva (UE) 2022/2555, che ha sostituito il quadro di riferimento in materia, al fine di tenere conto di una crescente digitalizzazione del mercato interno e di un panorama in evoluzione delle minacce alla cybersicurezza. Vi è una convergenza di obiettivi, dunque, fra i due provvedimenti e non la sovrapposizione, come alcuni colleghi hanno dichiarato in Commissione.

Il provvedimento in esame risponde perciò in modo adeguato ed efficace alla complessità e rapidità degli scenari di crisi e di minacce, rafforzando il ruolo istituzionale dell'ACN, anche in relazione alle sfide dell'attuale contesto, caratterizzato da nuove tipologie di confronto ibrido.

Per comprendere quanto sia necessaria l'approvazione di questo provvedimento, ritengo sufficiente ricordare i dati che il Sottosegretario Alfredo Mantovano ha fornito in Commissione. In particolare, nel 2023, l'Agenzia per la cybersicurezza istituita dal Governo Draghi ha trattato 1.411 eventi, circa 117 al mese, con un notevole incremento rispetto ai dati del 2022. Ricordo che per "evento", in questo caso, si intende un avvenimento che ha un impatto su almeno un soggetto nazionale e che comporta un *alert* e un successivo intervento di rimedio nei confronti dei soggetti colpiti.

In questo scenario di crisi geopolitica internazionale la tecnologia può essere usata anche da potenze straniere per raggiungere diversi e convergenti obiettivi; obiettivi che si possono realizzare mettendo in atto una duplice tipologia di eventi: eventi cosiddetti di DDoS, che pure in quest'ultimo anno e mezzo si sono verificati con attacchi *web* che mirano a fare danni, materiali o di immagine, prevalentemente orchestrati da gruppi *cyber* di attivisti filorussi o, da ultimo, filopalestinesi, che intervengono con una certa sincronia rispetto alle relative prese di posizione delle istituzioni nazionali in merito alla guerra in Ucraina o alla situazione in Israele; ed eventi cosiddetti *ransom* che rappresentano la versione informatica dell'estorsione, realizzata attraverso la sottrazione di informazioni sensibili, che colpisce piccole e medie aziende, aziende sanitarie locali, ma anche privati cittadini che, dinanzi al rischio di veder divulgati i propri dati personali, preferiscono pagare quanto viene loro richiesto piuttosto che denunciare il reato.

Se la pandemia è stata un acceleratore per la trasformazione digitale degli Stati, delle procedure, del trasferimento abnorme di attività, sia pubbliche sia delle imprese, sul *web*, al tempo stesso, questo fenomeno non è stato accompagnato dalla messa in sicurezza dei dati che vengono trasferiti su di esso. Il nostro Governo ha perciò giustamente deciso di intervenire con determinazione. L'impianto normativo vigente è ormai obsoleto, vecchio di vent'anni, che nel campo dell'informatica e della tecnologia equivale a certificarne l'inefficacia totale.

Come ha ben ricordato in Commissione sempre il Sottosegretario Mantovano, oggi, è più conveniente introdursi nei dati di una ASL per acquisire migliaia di dati sanitari e chiedere in Bitcoin una somma ingente per non diffonderli, oppure estrarre dati sensibili da una banca dati istituzionale, con gravi contraccolpi

istituzionali, piuttosto che realizzare un furto in una singola abitazione.

L'altro dato sul quale occorre riflettere per comprendere l'importanza di approvare il presente disegno di legge e proseguire con determinazione a sviluppare e a diffondere, a tutti i livelli dell'apparato pubblico statale e non, il concetto della cybersicurezza e l'adozione di procedure e metodiche sempre più efficaci nel contrastare i cybercriminali, è il dato fornitoci in audizione dal direttore del servizio di Polizia postale e delle comunicazioni, che ci ha comunicato che l'Interpol stima in 10,5 trilioni di dollari il costo globale del cybercrimine, numeri che non possono non destare enorme preoccupazione.

Il testo oggi all'esame dell'Aula risponde, a nostro avviso, anche dopo il lavoro importante svolto in Commissione, alle esigenze di sicurezza e a incrementare con procedure di *alert* e tempi certi una maggiore consapevolezza del rischio *cyber*, a superare comportamenti ingenui e debolezze, ad adottare misure organizzative adeguate, a dotarsi di una *governance* centralizzata degli aspetti di sicurezza e a innalzare le pene.

A chi parla di scarsità di risorse, occorre ribadire che, oggi, il punto non è tanto aggiungere risorse ai 50 milioni di euro all'Agenzia per la cybersicurezza nazionale, già previsti nell'ambito del Piano nazionale di ripresa e resilienza, alla Missione 1, Componente 1, quanto indirizzare, grazie a provvedimenti normativi, come quello di cui oggi discutiamo, quelle risorse già esistenti in chiave preventiva. Se, poi, in futuro si riusciranno a stanziare più risorse ben venga, ma al momento è opportuno certamente utilizzare al meglio quelle già stanziate e sufficienti.

Oltre a norme che impongono obblighi, è necessario predisporre strumenti che consentano agli enti e alle imprese di mappare le proprie vulnerabilità e di conoscere da dove possono venire le minacce, con l'obiettivo di fornire una guida concreta per la prevenzione, il rilevamento precoce, la risposta efficace e la ripresa rapida in caso di attacchi informatici. Questo testo, arricchito dagli emendamenti approvati in Commissione, rafforza tanto la risposta penale alle minacce alla sicurezza informatica quanto la resilienza della pubblica amministrazione, anticipando in un certo qual modo, mettendo un punto fermo nazionale, prima dell'attuazione della direttiva (UE) 2022/2555. Il nuovo articolo 8, infatti, introduce l'obbligo per i soggetti di cui all'articolo 1, comma 1, che a breve indicherò puntualmente, di individuare una struttura preposta all'attività di cybersicurezza, istituita *ex novo*, oppure individuata fra le strutture già esistenti.

Questa struttura sarà chiamata a sviluppare politiche e procedure di cybersicurezza; a elaborare e aggiornare il piano per il rischio *cyber*, nonché il documento interno relativo all'organizzazione e ai ruoli del sistema per la cybersicurezza informativa; a pianificare e attuare interventi di potenziamento della capacità gestionale del rischio *cyber* e delle misure previste dalle linee guida emanate dall'Agenzia per la cybersicurezza nazionale, nonché monitorare e valutare le minacce alla cybersicurezza dei propri sistemi informativi.

Riteniamo che questa scelta possa rappresentare un efficace strumento per mettere a terra il principio della resilienza cibernetica, a livello di pubblica amministrazione diffusa e non solo centrale. Infatti, questo disegno di legge, a maggior ragione dopo gli emendamenti in Commissione, dispone obblighi e fissa obiettivi, come detto in precedenza, non solo per le pubbliche amministrazioni centrali ma anche - e vediamo l'articolo 1, comma 1, come modificato in Commissione - per le regioni e le province autonome di Trento e di Bolzano, per le città metropolitane, i comuni con popolazione superiore ai 100.000 abitanti e, comunque, tutti i comuni capoluogo di regione, nonché per le società di trasporto pubblico urbano con bacino di utenza non inferiore ai 100.000 abitanti, per le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e le aziende sanitarie locali.

Tra i soggetti destinatari di queste norme

sono, altresì, comprese le rispettive società *in house* degli enti appena richiamati, che forniscono servizi informatici, di trasporto ovvero di raccolta, smaltimento e 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 e, inoltre, le società di gestione dei rifiuti, come definite ai sensi dell'articolo 3, punto 9, della direttiva 2008/98 del Parlamento europeo e del Consiglio.

Il disegno di legge, inoltre, interviene anche sul contrasto a fenomeni come quello recentemente assurto alle cronache di dossieraggio e spionaggio, e questo è ben evidenziato anche nella rubrica riformulata dell'articolo 8, che ora recita: "rafforzamento della resilienza delle pubbliche amministrazioni, referente per la cybersicurezza e rafforzamento della sicurezza delle modalità di accesso a banche dati pubbliche". Alla modifica della rubrica corrispondono, nell'articolato, strumenti e metodiche all'altezza della sfida di contrasto a queste attività illecite, molto pericolose per la sicurezza nazionale e per il possibile inquinamento della democrazia e della pubblica opinione che da queste può derivare. Metodi e procedure tecnologicamente innovative, affiancate da sanzioni robuste ed adeguate alla gravità degli illeciti.

Concludo, onorevoli colleghi. Ho voluto evidenziare, in questo mio intervento, solo alcuni dei molti punti trattati dall'A.C. 1717-A, la cui condivisione degli obiettivi è certamente generale e ampia. Sollecito l'urgenza che il Parlamento approvi queste misure, per rinnovare un impianto non più adeguato a dare risposte efficaci.

Per vincere la sfida della cybersicurezza e per contrastare la cybercriminalità occorrono norme adeguate, tecnicamente performanti ed efficaci e, soprattutto, diffondere a ogni livello istituzionale la cultura della cyber-resilienza. È fondamentale che il Governo, la pubblica amministrazione, il settore privato e i cittadini si sentano tutti coinvolti nell'affrontare questa nuova sfida dell'era digitale, per garantire un futuro più sicuro per tutti *(Applausi dei deputati del gruppo Fratelli d'Italia)*.

PRESIDENTE. È iscritto a parlare l'onorevole Casu. Ne ha facoltà.

ANDREA CASU (PD-IDP). Grazie, Presidente, onorevoli colleghi, onorevoli rappresentanti del Governo. Innanzitutto, vorrei aprire questo intervento lanciando da quest'Aula, a nome del gruppo del Partito Democratico, ma spero di tutti i gruppi, un forte messaggio di vicinanza, di solidarietà, di sostegno al sindaco Roberto Gualtieri per le accuse e le minacce che ha subito, proprio nella giornata di oggi. È stato minacciato sui *social* dopo aver presentato un progetto di rigenerazione urbana, nel quartiere di Tor Bella Monaca, con forme di odio molto forti che sono state espresse nei suoi confronti.

È importante che, di fronte a questo tipo di odio che nella rete si sviluppa in maniera molto forte e netta, ci sia una risposta solidale di tutte le istituzioni. La battaglia contro la criminalità organizzata, che sta portando avanti l'amministrazione in Campidoglio, in VI Municipio, in tutta la città, è una battaglia che deve vedere tutte le istituzioni unite. Questi messaggi - adesso per non far pubblicità non li ripeterò - danno il senso anche di come spesso l'odio sulla rete vada molto veloce. Si parlava, nell'intervento che mi ha preceduto, di cultura, della capacità di essere resilienti nei confronti dei cyberattacchi, della cultura della cybersicurezza.

Ciò a cui, però, purtroppo, assistiamo è un'idea, distorta, di impunità nella dimensione digitale, cioè del fatto che ciò che viene commesso nella dimensione digitale sia diverso e abbia conseguenze in qualche modo meno gravi o che possa incidere in misura minore rispetto a quello che avviene nella dimensione non digitale del nostro agire e del nostro vivere, e questo non è vero. È stato negato da tutti i dati che sono stati citati oggi: non è vero per la vita economica, non è vero per la vita

relazionale, non è vero semplicemente perché ormai la nostra vita si sviluppa in un *continuum* di spazi fisici e digitali.

Ora, per questo, in apertura del mio intervento voglio fare un esempio. Stiamo ancora affrontando il provvedimento, lo abbiamo visto in Commissione, avremo l'occasione - mi auguro - di poter correggere ulteriormente in Aula alcuni passaggi fortemente critici e preoccupanti su cui ci siamo confrontati. Però, vi vorrei fare un esempio per aprire questa riflessione comune, che vorrei portare avanti in discussione generale. Se oggi avessimo di fronte un decreto che non si occupasse di cybersicurezza ma di sicurezza e ci fossero una serie di nuovi impegni (sono stati ricordati negli interventi) e di nuovi oneri non solo per le amministrazioni centrali ma anche per le regioni, per le città metropolitane, per le province, per i comuni e ci fossero delle cose molto importanti che stiamo andando a cambiare, per rendere più sicure le nostre strade, per rendere più sicure le attività vicino alle nostre stazioni o da altre parti; se, alla fine di tutti questi oneri e impegni che andiamo a prevedere e a proporre, ci venisse detto che tutto ciò è "a invarianza finanziaria", penso che in quest'Aula tutti si alzerebbero e direbbero: ma com'è possibile garantire più sicurezza, mettere più persone che garantiscono la sicurezza, prevedere maggiori oneri e maggiori impegni a invarianza finanziaria? Significa che quelle risorse devono essere tolte da qualche altra parte; che non c'è più sicurezza se si dice "sorvegliamo meglio le stazioni", ma non si danno alla Polizia le risorse per poter essere presenti nelle stazioni o anche in altri luoghi; che non c'è maggiore sicurezza nel mondo, non digitale, ma nel mondo reale, nel momento in cui non si decide di dare un valore a questa maggiore sicurezza che cammina certamente sulle regole, sulle norme, sugli obblighi, sui divieti ma anche sulle risorse che si mettono a disposizione per fare sì che le norme vengano applicate.

Questo paradosso - che sarebbe di tutta evidenza se stessimo parlando di un decreto Sicurezza - c'è anche in un decreto sulla cybersicurezza, perché questo è il punto veramente dolente di questa discussione.

Per fare un esempio che spiega quanto questo sia il punto dolente - veramente, ringrazio ancora una volta gli uffici per il grande lavoro che fanno ogni giorno e, quindi, sarà molto facile per tutti noi poter ricostruire anche i passaggi in Commissione parlamentare, perché sono solo di pochi mesi fa - vi posso raccontare e ricordare quello che è avvenuto con la legge di delegazione europea.

La legge di delegazione europea anticipava già tutta una serie di disposizioni legate alla NIS 2 che, come è stato ricordato dai relatori, è arrivata perché evidentemente la NIS 1 non è stata sufficiente a garantire un miglioramento del livello di difesa del sistema comunitario e, allora, è stata necessaria una nuova direttiva. Quando è arrivata questa nuova direttiva ho presentato un emendamento per chiedere di innalzare i livelli di difesa, anche per quanto riguarda i comuni e le città metropolitane e l'abbiamo fatto in I Commissione. In I Commissione è passato perché c'è concordanza su questi temi, cioè sul fatto di garantire maggiore sicurezza ai dati dei comuni, che sono i nostri dati, evitando che l'Italia diventi la miniera d'oro dei dati personali anagrafici delle persone, con una banca dati di 60 milioni di persone facilmente accessibile e depredabile da parte di tutto il mondo. Quando lo abbiamo presentato, l'emendamento è stato approvato da tutta la Commissione. Era una legge di delegazione europea, non bastava il voto in I Commissione e siamo arrivati in XIV Commissione, in cui era presente la Sottosegretaria Siracusano. È stato approvato anche in XIV Commissione, quindi l'esame di merito si è esaurito e, a quel punto, doveva esserci un passaggio in V Commissione, in Commissione bilancio.

E quell'emendamento proponeva di anticipare la NIS 2 per i comuni e di fare in modo che quello che varrà per le banche dati, ad esempio dei sistemi sanitari regionali, valga

anche per le banche dati anagrafici dei comuni; quell'emendamento che avevo presentato, con un parere favorevole di maggioranza e di opposizione e del Governo, è stato cassato dalla Commissione bilancio, perché la stessa ha detto che non si poteva prevedere questo adempimento in un provvedimento a invarianza finanziaria.

Quindi, ciò che noi stiamo per votare adesso, all'articolo 18, prevedendo questi oneri a invarianza finanziaria, è quello contro cui ci siamo espressi solo pochi mesi fa, quando lo abbiamo chiesto, nell'ambito dell'esame della legge di delegazione europea, che andava a recepire la NIS 2; proprio per tutelarci da questo punto di vista, avevamo inserito alcuni principi e clausole di salvaguardia, con un principio di adeguatezza, di proporzionalità, che poteva essere - in qualche modo - orientabile sulla base del tipo di risorse che venivano messe a disposizione.

Quindi, delle due l'una: o si intende - ma allora c'è un cambiamento rispetto a quello che si è fatto solo fino a pochi mesi fa - che, intanto, si fanno le norme e poi si troveranno le risorse per applicarle, oppure - se questo deve essere contestuale - significa che bisogna legare i provvedimenti che noi mettiamo in questo decreto - che, in larga parte, condividiamo, abbiamo sostenuto e stimolato con i nostri emendamenti - a quella dotazione di risorse che serve per metterli in pratica. Da questo punto di vista, noi abbiamo fatto anche delle proposte che non hanno nemmeno oneri aggiuntivi. Ne faccio solo un esempio: è stato ricordato che c'è una quota per la difesa *cyber* dei fondi del PNRR e, allora, noi abbiamo chiesto che almeno i ribassi d'asta della parte digitale dei bandi del PNRR possano essere utilizzati per rimpinguare la dotazione della parte per la cybersicurezza. Poniamo questo tema perché le grandi democrazie, i grandi Paesi che stanno affrontando a viso aperto la sfida digitale destinano un quantitativo di risorse sul tema della cybersicurezza molto più significativo del nostro, sia in termini di rapporto col prodotto interno lordo, sia in termini di rapporto rispetto alla leva complessiva degli investimenti digitali che vengono fatti. Negli Stati Uniti, ad esempio, dei 65 miliardi di investimenti nel digitale, 11 miliardi sono sulla cybersicurezza. Da noi questo rapporto non c'è. E cosa genera questo squilibrio? Genera che noi acceleriamo nella digitalizzazione, ma non rendiamo - nell'effettivo, non solo nei principi su carta, ma nella realtà - più sicuro questo scenario. E cosa succede? Succede quello che abbiamo visto. Una percentuale pari quasi al 100 per cento, il 99 per cento delle imprese, negli ultimi anni hanno subito almeno un attacco. Quando si parla di un attacco, ci sono piccoli attacchi, ma - si citava prima - in esponenziale crescita è il *ransomware*, l'attacco per riscatto: viene bloccato il portale di una piccola-media impresa - non parliamo, infatti, solo delle grandi imprese, ma anche delle piccole e delle medie imprese, che sono un elemento fondamentale del nostro tessuto - e impedito di operare e di lavorare, a meno che non si paghi quel riscatto. Quanti pagano questo riscatto? Troppi. Quanto enorme è quel costo, di cui tutto il nostro sistema si fa carico?

Per non parlare poi del rischio a cui andiamo incontro ogni giorno. Adesso noi valuteremo e capiremo. Sono anche allarmanti alcuni dati, proprio delle ultime settimane, circa l'utilizzo che si sta facendo, in un anno che sarà decisivo per il mondo; votano Paesi importanti, votano miliardi di persone in quest'anno, vota l'Europa, votano gli Stati Uniti e non solo: saranno le prime elezioni in cui, con una così forte profilazione di *cyber* attacchi, noi avremo anche un processo democratico. Da questo punto di vista, è indispensabile alzare gli scudi del nostro sistema difensivo nazionale ed europeo, ma, per farlo, gli strumenti devono essere concreti ed effettivi.

Io sono preoccupato da un fatto: aver previsto questi princìpi senza avere dato garanzie sulle risorse che servono a metterle in pratica può valere, sicuramente, per annunciare di aver fatto qualcosa, ma potrebbe anche creare alcuni effetti distorsivi. Il primo è che un'amministrazione, un comune, che già

fatica tantissimo a garantire i servizi essenziali, per poter adempiere ai nuovi obblighi e ai nuovi adempimenti, per potere assumere quel personale che sarà indispensabile, cosa dovrebbe fare? Tagliare da qualche altra parte? Cosa possiamo chiedergli? Di tagliare dagli asili nido, per avere più risorse per la cybersicurezza?

Ecco, questo non è pensabile, non è ammissibile. Serve mettere in campo un complesso di risorse adeguato. Abbiamo fatto alcune proposte, il Governo può anche decidere di andare in direzione diversa dalle proposte che abbiamo avanzato ai nostri emendamenti, ma sfuggire alla necessità di dare a questi oneri una copertura è, a nostro avviso, molto preoccupante e molto problematico.

Non solo, ci sono altri aspetti che abbiamo evidenziato. Io voglio ringraziare la Sottosegretaria e il Governo, per aver assunto un impegno in Commissione, quello di trovare insieme la riformulazione più adatta. È chiaro, questo è un provvedimento che riguarda alcune Commissioni. Prima che nascesse questo provvedimento, io ho seguito il tema in IX Commissione (che ha competenza sulle comunicazioni). Questo provvedimento è stato attribuito alla I Commissione e alla II Commissione, quindi ci sono altri profili, soprattutto profili di giustizia. Con grande umiltà, non entro negli aspetti più squisitamente giuridici, ma chiedo una considerazione pratica e un impegno del Governo in tal senso, che venga onorato nell'Aula, nella giornata di domani.

Nelle audizioni che abbiamo svolto, noi abbiamo posto il tema della cosiddetta legittima difesa da un punto di vista di *cyber* attacchi. Possiamo non chiamarla legittima difesa, possiamo chiamarla difesa oppure come si ritenga più utile, però, il punto è molto semplice e molto chiaro: se i sistemi tecnologici per difendersi che oggi vengono utilizzati sono sistemi che prevedono come forma di difesa anche la capacità di bloccare l'offendente, è chiaro che il sistema difensivo ha una componente difensiva atta, potenzialmente, a offendere. Non può essere il semplice fatto di possedere un sistema che può potenzialmente offendere, se quel sistema è lo stesso che serve anche a difendersi e viene utilizzato per scopi esclusivamente difensivi, a essere passibile di sanzioni penali. Altrimenti, il paradosso che stiamo generando è che noi, per difenderci da *cyber* attacchi che arrivano da fuori dei nostri confini, disarmiamo la difesa. In altre parole, stiamo creando le condizioni per cui chi si difende, comprando un programma con cui difendersi e allo stesso tempo contrattaccare, di fatto, è passibile di sanzioni - e quindi non può essere utilizzato in Italia - ma non facciamo nulla per fermare chi ci sta attaccando.

È chiaro che nessuno debba, nel nostro Paese, compiere azioni ostili, però, è anche vero che, nel nostro Paese, deve essere garantita, come negli altri paesi europei e nei grandi paesi, la possibilità di difendersi dai *cyber* attacchi con le soluzioni tecnologicamente più avanzate. Naturalmente, noi siamo aperti a ogni tipo di riformulazione e di chiarimento, che sgombri il campo da qualunque equivoco o possibile interpretazione che stravolga questo principio, e che si esplichi nei confronti di attacchi che noi vogliamo assolutamente combattere in ogni sede, in ogni luogo, in ogni latitudine e in ogni longitudine. Però, è anche vero che, se da argomentati interventi, interlocuzioni e sollecitazioni, che abbiamo avuto durante le audizioni, emerge un serio rischio, non solo di non rendere più difficile la vita a chi ci attacca, ma anche di rendere più difficile la vita a chi vuole difendersi in Italia, perlomeno dobbiamo alzare lo sguardo e cercare di capire come inserire una riga - demandando a quello che sarà il compito dell'ACN o dei soggetti che sono chiamati a interpretare questo principio - sgombri il campo da questo dubbio e da questa perplessità.

Così come è importante - è stato ribadito - un ruolo che va potenziato. Noi abbiamo presentato emendamenti per un potenziamento del ruolo dell'ACN, dell'assetto istituzionale di cui noi ci stiamo dotando per fronteggiare questa grande emergenza nazionale dei *cyber*

attacchi; penso che ciò sia giusto. Da un certo punto di vista, serve anche a sanare alcuni problemi che avevamo avuto. Faccio l'esempio della crittografia, sul quale abbiamo presentato emendamenti e sul quale c'è stata un'occasione di approvazione di alcuni emendamenti e alcune riformulazioni, anche condivise da parlamentari di opposizione, di maggioranza e di varie forze, a dimostrazione di quanto questo fosse un tema trasversale. C'era una formulazione del codice delle comunicazioni elettroniche da un punto di vista della crittografia che, in certi passaggi, non era tecnologicamente ammissibile. Rischiavamo di vietare la crittografia in Italia e consentirla da altre parti, a determinate caratteristiche. Questo rischio, che era presente nel codice delle comunicazioni elettroniche, non era presente nelle linee guida dell'ACN, che, invece, chiarivano molto chiaramente come si doveva procedere. Da questo punto di vista, abbiamo posto una domanda nell'ambito delle audizioni e presentato alcuni emendamenti.

Questi emendamenti sono stati approvati e - almeno da questo punto di vista - si è sanato un aspetto e ci potrà essere un sistema equilibrato, che deve richiedere che norme molto complesse e complicate, che si stanno scrivendo in un contesto che si sta evolvendo mentre noi lo affrontiamo, siano in grado di avvicinarsi il più possibile all'obiettivo per cui vengono portate avanti.

È chiaro che c'è una componente anche di difficoltà, di rischio, di problematicità nel procedere in uno scenario in così rapida evoluzione, ma è fondamentale che, proprio di fronte a sfide come questa, un sistema Paese sia in grado, al di là delle differenze, di cogliere l'importanza strategica, di cogliere le priorità e di agire in maniera conseguente.

Non interverrò su ogni singolo punto, ci sarà poi l'occasione nell'ambito dell'esame degli emendamenti. Noi abbiamo ripresentato in Aula gli emendamenti che avevamo presentato in Commissione, nella speranza che possano essere accolti, o direttamente o attraverso riformulazioni.

Non entrerò nello specifico di alcune formulazioni che hanno aperto una serie di interrogativi - che spero possano essere sanati dal Governo nelle prossime ore - circa i vari aspetti. Mi limiterò a rivolgere, ancora una volta, da questa ala, questo appello: il valore che si attribuisce ad alcune politiche è fatto da tante componenti, ma una componente essenziale è il valore delle risorse che si decide di destinare a un tema.

Non si può dire, nello stesso momento, che la cybersicurezza è un'emergenza nazionale, che la cybersicurezza richiede più interventi, più oneri, più impegni da parte di tutti i livelli istituzionali e poi prevedere che tutto questo aumento di oneri, di impegni, valga zero. Perché significa che si dà alla cybersicurezza valore zero euro.

Noi siamo convinti, invece, che questo non possa avvenire, così come non avviene nei grandi Paesi, che, a differenza nostra, riescono a crescere nella digitalizzazione e, al tempo stesso, a crescere nella capacità di proteggersi nel mondo digitale. Al contrario, noi cresciamo nella digitalizzazione e perdiamo rovinosamente posizioni da un punto di vista degli attacchi gravi che subiamo ogni giorno, che, come abbiamo visto, mettono fortemente a rischio tanti aspetti, a partire dagli aspetti democratici fino ad arrivare agli aspetti della sicurezza dei nostri dati personali, agli aspetti economici e sociali e alle imprese, anche piccole e medie. Da questo punto di vista, noi auspichiamo che ci possa essere un cambiamento e che questo cambiamento possa avvenire già domani, con il superamento di un principio che rischia veramente di fare sì che questo provvedimento garantisca solo su carta un miglioramento sotto il profilo della difesa stabile del Paese, senza però mettere in campo gli strumenti per fare sì che detta difesa si realizzi nella società.

PRESIDENTE. È iscritto a parlare l'onorevole Bicchielli. Ne ha facoltà.

PINO BICCHIELLI (NM(N-C-U-I)-M). Signor

Presidente, onorevoli colleghi, signora Sottosegretaria Siracusano, se c'è un insegnamento da trarre dal susseguirsi delle crisi degli ultimi anni è la necessità di ridurre la dipendenza dall'estero, in particolare nei settori nevralgici. Lo abbiamo visto con l'energia: le forniture di approvvigionamenti essenziali per le famiglie e le imprese sono stati utilizzati come armi di pressione nell'ambito delle tensioni che hanno colpito il cuore dell'Europa.

Sicurezza: sicurezza è una parola che richiama al contempo tranquillità e il suo contraltare, ovvero il rischio, il pericolo, perché la sicurezza va difesa e preservata, riducendo l'esposizione e aumentando le protezioni. Oggi un terreno su cui non mancano minacce alla sicurezza nazionale è sicuramente il digitale. Gli attacchi alle reti e ai sistemi e al loro funzionamento, il furto di dati sensibili, sono crimini informatici che a volte possono rappresentare veri e propri atti terroristici o di guerra, se orientati a danneggiare o distruggere servizi essenziali a livello nazionale. In una fase come questa, in cui il passaggio al digitale delle informazioni e dei processi è sempre più massivo, diventa quindi cruciale il rafforzamento della cybersicurezza nazionale e l'adeguamento delle norme per il contrasto e il perseguimento dei reati informatici. Ma il punto su cui intendo richiamare la vostra attenzione è quello che ho accennato in apertura del mio intervento: la necessità di ridurre la dipendenza dall'estero. Le maggiori dipendenze strutturali, a livello europeo, riguardano Stati Uniti e Cina, in diversi settori che coinvolgono piattaforme digitali e infrastrutture di telecomunicazioni.

All'indomani della crisi pandemica, il tema della sovranità tecnologica è entrato a far parte del dibattito dell'agenda europea e nazionale, riferendosi, con questo termine, alla capacità dell'Unione di sviluppare, produrre e mantenere le proprie tecnologie critiche senza dipendere da altri Paesi. Sono tre le fasi da controllare, ossia la ricerca, l'innovazione e la *skill up*: la ricerca, ovvero la capacità di generare nuove idee, scoperte e brevetti; l'innovazione, cioè la capacità di trasformare la ricerca in prodotto; la *skill up*, ossia la capacità di far crescere e consolidare le *startup* innovative.

La Cina possiede quasi il doppio degli operatori nel settore dell'intelligenza artificiale rispetto all'Unione europea, posizionandosi non molto distante dagli Stati Uniti. È quanto emerge dal *report* della Commissione europea del gennaio di quest'anno. La supremazia cinese nei settori delle nuove tecnologie, come sottolinea il *report* stesso, rende l'Europa vulnerabile a dinamiche negative, che influenzano la competitività, la catena di approvvigionamento, ma anche l'ambito della definizione degli standard internazionali e mi riferisco non solo a quelli tecnologici, ma anche a quelli etici. Si pensi allo sviluppo, ad esempio, dell'intelligenza artificiale e ai molteplici quesiti che solleva la sua applicazione.

Signor Presidente, arranchiamo, purtroppo, ancora soprattutto nella capacità di convertire la ricerca e l'innovazione in *startup*. All'inizio del 2023, l'Unione europea contava solo 249 unicorni, cioè quelle *startup* valutate oltre un miliardo di dollari, rispetto alle 1.444 degli Stati Uniti e alle 330 della Cina.

Sebbene l'Unione, a partire dal 2010, abbia superato la Cina nel numero di unicorni nei settori dell'energia pulita e delle biotecnologie, nel campo del digitale e dell'elettronica, in particolar modo nell'intelligenza artificiale e nella *deep tech*, la Cina detiene un vantaggio considerevole. Questo impone, quindi, una strategia complessiva per il rafforzamento della cybersicurezza che tocca molteplici aspetti, anche di tipo industriale. In tal senso, quindi, la definizione del perimetro nazionale di *cybersecurity* è funzionale anche allo sviluppo di un tessuto industriale, tecnologico e orientato alla sicurezza informatica. Penso, ad esempio, alla disciplina dei contratti pubblici di beni e servizi informatici, prevista dall'articolo 10 del provvedimento in esame, e alla valorizzazione dell'intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale, anche al fine di favorire un uso etico e corretto dei sistemi basati sull'intelligenza artificiale, in un rapporto funzionale reciproco. L'intelligenza

artificiale e le sue infinite possibilità di sviluppo e applicazione rappresentano tanto una risorsa quanto un rischio per la sicurezza cibernetica nazionale e, in questa duplicità, vanno affrontate e gestite.

L'Osservatorio del Politecnico di Milano, nel suo ultimo *report* di febbraio del 2024, ha registrato un'ulteriore crescita del mercato dell'intelligenza artificiale in Italia. Nel 2023, ha segnato un più 52 per cento, raggiungendo il valore di 760 milioni di euro, dopo che già nel 2022 aveva registrato un più 32 per cento rispetto all'anno precedente. La gran parte degli investimenti riguarda soluzioni di analisi e interpretazione di testi per ricerca semantica di classificazione, sintesi e spiegazione di documenti o agenti conversazionali tradizionali, mentre sono ancora limitati al 5 per cento, pari quindi a circa 38 milioni di euro, i progetti di *generative* AI. Sei grandi imprese italiane su dieci hanno già avviato un qualche progetto di intelligenza artificiale, almeno a livello di sperimentazione, ma ben due su tre hanno già discusso internamente dell'applicazione della *generative* AI e tra queste una su quattro ha avviato una sperimentazione.

Questi dati, signor Presidente, ci danno il senso di un tessuto industriale vitale, ma impongono, al contempo, anche l'urgenza di combinare cybersicurezza e sviluppo tecnologico. In quest'ottica, è positiva l'approvazione, nel Consiglio dei ministri del 23 aprile scorso, del ddl in materia di intelligenza artificiale, che accompagna l'introduzione dell'AI Act, approvato dal Parlamento europeo il 13 marzo di quest'anno. Sono tutti strumenti, signor Presidente, che è necessario e urgente mettere in campo per puntare alla sovranità tecnologica, essenziale al rafforzamento della sicurezza cibernetica nazionale. Come Noi Moderati siamo, dal primo giorno di questa legislatura, attenti sia alle potenzialità sia ai rischi che corrono il nostro Paese e ognuno dei suoi cittadini.

Proprio per questo, stiamo portando avanti con determinazione e costantemente le nostre istanze, tese ad un cambiamento non solo normativo, ma soprattutto culturale su un tema strategico per il futuro del nostro Paese.

PRESIDENTE. È iscritto a parlare l'onorevole Dori. Ne ha facoltà.

DEVIS DORI (AVS). Anzitutto, come Alleanza Verdi e Sinistra, esprimiamo solidarietà al sindaco Gualtieri per le gravi e inaccettabili minacce ricevute via *social*. Non è un caso che sia stato proprio minacciato per alcune azioni di rigenerazione urbana a Tor Bella Monaca, perché sappiamo che il degrado alimenta l'illegalità e la criminalità. Quindi, c'è chi vuole il degrado, mentre la riqualificazione urbana è uno strumento di lotta all'illegalità. Per questo motivo, ribadisco la solidarietà al sindaco di Roma.

Il provvedimento che approda oggi in Aula è volto a rafforzare la cybersicurezza nazionale. Pertanto, si tratta di un disegno di legge condivisibile nelle finalità e negli intenti, ma poi presenta criticità rispetto alle modalità con le quali si intendono raggiungere quegli obiettivi. Poi, ci sono alcune carenze che nemmeno la fase emendativa in Commissione ha saputo colmare.

La sicurezza informatica è un tema ineludibile. Il progressivo intensificarsi di attacchi di diversa natura, finalizzati alla messa fuori uso di sistemi informativi o all'estrazione fraudolenta dei dati, rende certamente necessario un rafforzamento delle difese cibernetiche, da attuarsi a livello regolamentare e, conseguentemente, operativo a tutti i livelli. Quindi, siamo certamente d'accordo sulla necessità di un intervento. Tuttavia, nel testo che approda oggi in Aula ci sono alcuni elementi per noi di grave criticità.

Il primo, evidenziato anche dai colleghi che mi hanno preceduto, è l'assenza di fondi: non si può fare un provvedimento di questa natura a costo zero. Poi, c'è una mancanza di chiarezza sulla formazione *cyber* dei dipendenti pubblici: è tutto troppo fumoso. Inoltre, sarebbe stata necessaria un'assunzione anche di esperti specifici in materia di cybersicurezza.

Una buona parte del provvedimento si concentra, invece, sull'aumento delle sanzioni di natura amministrativa o penale che, per quanto possano avere anche un minimo effetto di deterrenza, certamente non sono in grado di impedire atti illegali, compiuti in particolare all'estero. Le sanzioni, se arrivano e quando arrivano, arrivano sempre troppo tardi, quando il danno, purtroppo, è stato fatto. Quindi, la condivisibile esigenza di implementare le sovrastrutture di sicurezza, a presidio dei sistemi pubblici e privati di cibernetica, che ispira questo disegno di legge - per rispondere proprio alla crescente offensività delle aggressioni realizzate con mezzi informatici e telematici verso gli apparati statali - non richiedeva, però, di intervenire necessariamente sul sistema sanzionatorio penale.

Come evidenziato nel Rapporto Clusit 2024, che lamenta un incremento significativo in Italia degli attacchi gravi globali (l'11 per cento nel 2023 rispetto al 7,6 per cento del 2022, per un totale di 310 attacchi), il nostro Paese appare sempre più nel mirino dei cybercriminali e necessita, quindi, di un adeguamento delle dotazioni di sicurezza preventiva degli apparati pubblici e privati, proprio per scongiurare il rischio di collasso del sistema.

D'altra parte, il complesso delle norme del disegno di legge affida il raggiungimento dell'obiettivo della sicurezza cibernetica interna alla risposta repressiva dei fenomeni criminali, con nuovi reati e un aumento significativo delle pene. Il rischio, però, è di non centrare l'obiettivo e lo scopo. Proprio per questi reati, infatti, gli strumenti investigativi appaiono il più delle volte insufficienti ad identificare gli autori, magari nascosti dietro reti VPN allocate in Paesi ombra. Ciò rende davvero inefficace la deterrenza della sanzione penale, rispetto a processi di difficile costruzione anche probatoria. Il dubbio, quindi, circa la bontà e l'efficacia di tale intervento repressivo, rispetto all'ampiezza e la complessità del fenomeno criminale, induce proprio alcune riflessioni rispetto al fatto di concentrare gli sforzi su processi preventivi di adeguamento dell'apparato di sicurezza.

Per carità, ben venga anche la parte della deterrenza della sanzione penale, laddove davvero è necessaria. Però, bisognava fare un investimento preventivo e qui i fondi - ribadisco nuovamente - non ci sono. Quindi, non si può delegare tutto alla proliferazione di nuove fattispecie di reato, come abbiamo già visto in altre occasioni. Perché, a quel punto, l'impressione è che questi provvedimenti abbiano un carattere meramente simbolico. Ciò risulta dimostrato nei fatti.

Per quanto riguarda la carenza di fondi, si aggiungono nuovi compiti per le pubbliche amministrazioni, così come per altri soggetti privati, e quindi c'è una necessità di individuare dei relativi referenti, senza però che a tali compiti corrispondano gli strumenti economici per formarli e per acquisire le competenze, e personale adeguato per prevenire e reagire agli attacchi.

Basti 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 cibernetica. Sebbene sul tema della cybersicurezza siano comunque stanziate risorse in legge di bilancio o nel PNRR, queste non sono destinate alla finalità di questo provvedimento. E, comunque, a detta di numerosi soggetti auditi, le risorse previste dai bandi dell'Agenzia nazionale per la cybersicurezza sono del tutto insufficienti, anche in caso fossero stati soltanto raddoppiati.

Si rammenta come l'Italia è 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 della Francia e della Germania, dello 0,29 per cento del Regno Unito e dello 0,34 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.

Per quanto riguarda, invece, gli

emendamenti che abbiamo valutato e studiato nelle due Commissioni riunite, dobbiamo registrare, da un lato, un miglioramento e, dall'altro, un peggioramento. Mi riferisco, per l'aspetto migliorativo, all'abrogazione dell'articolo 7 del disegno di legge che, nella sua formulazione originaria, avrebbe attribuito all'Agenzia per la cybersicurezza nazionale compiti in materia di intelligenza artificiale. Anzi, leggo testualmente, il compito sarebbe stato quello di "favorire un uso etico e corretto dei sistemi basati su tale tecnologia". Però, il tema dell'intelligenza artificiale è estremamente complesso e non può essere certo affrontato in maniera superficiale. Quindi, in questo ambito servirà un provvedimento *ad hoc*, con il forte coinvolgimento del Parlamento, visto che si vanno a toccare anche certi diritti della persona. Accogliamo certamente con favore il fatto che il Governo abbia accettato, anche su richiesta delle opposizioni e su suggerimento degli auditi, di togliere il tema da questo provvedimento, considerato che il tema della cybersicurezza e quello dell'intelligenza artificiale hanno, sì, alcuni punti di contatto, ma non sono affatto sovrapponibili. Necessitano di una trattazione *ad hoc* separata.

Motivo, invece, di estrema preoccupazione per noi è l'introduzione nel disegno di legge, in fase emendativa, dell'articolo 22, con un emendamento, volto a modificare l'articolo 7 della legge n. 1311 del 1962, prevedendo la possibilità per gli ispettori del Ministero della Giustizia - quindi, un organo di natura amministrativa e non giurisdizionale - di verificare - leggo testualmente il nuovo articolo 22 introdotto nel disegno di legge - "il rispetto delle prescrizioni di sicurezza negli accessi nelle banche dati in uso presso gli uffici giudiziari". Ecco, chiaramente, questo ha comportato un miglioramento.

Questa riformulazione rispetto al testo originario dell'emendamento - perché prima si parlava direttamente di verifica degli accessi, ora, almeno, si parla di rispetto delle prescrizioni di sicurezza - sembra sostanzialmente un po' una riformulazione "camomilla", cioè elaborata giusto per tenere calmi gli animi, mantenere tranquilla l'opinione pubblica e far credere che vada tutto bene, ma poi, nei fatti, anche con questa formulazione, a mio parere, non cambia nulla. Infatti, anche quella formulazione "rispetto delle prescrizioni di sicurezza negli accessi" cosa significa? Il Governo qui dovrebbe chiarire in maniera precisa il significato di queste prescrizioni di sicurezza. Quindi, chi elaborerà queste prescrizioni? Magari un decreto ministeriale? Pertanto, ci troveremo davvero di fronte a un corto circuito perché, se è il Ministero stesso a stabilire le regole per accedere ai *database* degli uffici giudiziari, da qui nasce la nostra preoccupazione. E sembra che, effettivamente, questa misura possa andare proprio nella direzione impressa dal Governo con vari provvedimenti, in particolare del Ministro della Giustizia, con strumenti di controllo politico nei confronti della magistratura, magari non nei confronti del singolo magistrato, ma in generale rispetto all'attività giudiziaria. Tutti abbiamo la preoccupazione che nessuno acceda illegalmente alle banche dati giudiziarie - anzi, proprio a quelle in particolare - però, poi bisogna trovare il metodo adeguato. In realtà, a nostro parere, questo non è lo strumento e apre un'ulteriore preoccupazione.

Per questo motivo, abbiamo presentato un emendamento per l'Aula, proprio per abrogare ed eliminare questo nuovo articolo 22. Speriamo, poi, che possa esserci un'ulteriore riflessione da parte del Governo.

Sul tema della cybersicurezza, sicuramente, servono anche uno sforzo e un percorso di natura culturale che portino, anche con un investimento economico nella formazione dei nostri giovani e degli studenti, ad un'attenzione e ad una sensibilità verso il tema della cybersicurezza, dell'uso corretto dei dispositivi digitali, facendone percepire i pericoli ma anche chiaramente l'uso responsabile.

Ecco, proprio in questa direzione serviranno sicuramente anche un intervento e un'interlocuzione con il Ministero dell'Istruzione, proprio per valorizzare, anche

nei percorsi didattici, l'approccio responsabile al mondo digitale.

Concludo, Presidente, ribadendo anzitutto che il nostro gruppo condivide l'obiettivo, la finalità di questo provvedimento, però siamo estremamente sorpresi che il Governo abbia avuto l'ardire di intervenire a costo zero su questo tema. Infatti, stiamo parlando sostanzialmente di difesa, quindi, salvo che questo Governo intenda la difesa soltanto di natura militare con le armi, noi probabilmente avremmo preferito che, già in questo provvedimento, fossero passati dei fondi su questa forma di difesa, perché anche questa è una forma di difesa, quella della cybersicurezza.

Sostanzialmente qui state facendo - lo dico in particolare al Governo, ma anche alla maggioranza - le nozze coi fichi secchi, ma, in questo modo, gli sposi rischiano di scappare prima delle nozze e sostanzialmente sul tavolo rimarranno solo quei fichi secchi. In particolare, poi, a farne le spese sarà la nostra cybersicurezza.

PRESIDENTE. È iscritta a parlare l'onorevole Matone. Ne ha facoltà.

SIMONETTA MATONE (LEGA). Grazie, Presidente. Mai una legge fu più necessaria, tempestiva e veloce di questa: è stata foriera di polemiche iniziali, per presunti attacchi liberticidi, poi finalmente queste polemiche si sono sopite per la ragionevolezza messa in campo da tutte le parti.

Perché è necessaria? Lo è per gli attacchi documentati dal CASA, che è un organo nato nel 2004 da una felice intuizione di De Gennaro e di Pisanu, che all'epoca crearono quest'agenzia particolare. È un luogo di confronto permanente tra Forze di polizia e di *intelligence*, ed è il cuore del comitato antiterrorismo. Secondo l'Agenzia, gli attacchi *cyber* sono cresciuti del 30 per cento nel 2023 rispetto al 2022, quelli di tipo criminale sono aumentati del 27 per cento e quelli di matrice politica del 625 per cento.

Sono assalti mirati per mandare in *tilt* portali e siti istituzionali e, nell'80 per cento dei casi, sono stati rivendicati da "hackeristi" filorussi e filopalestinesi. Le tecnologie di ultima generazione ci hanno trovato assolutamente indifesi - questo non lo dico io, ma lo dice il procuratore nazionale antimafia Melillo - e possono mettere in seria difficoltà i nostri apparati a causa del divario assolutamente evidente tra l'estrema capacità tecnologica di chi attacca e la nostra capacità di risposta.

Lo spazio virtuale è diventato il cardine degli interventi mirati delle reti criminali e soprattutto di quelle terroristiche. Sono state rassicuranti le parole del Ministro degli Esteri, Tajani, sul fatto che la NATO sia al sicuro da possibili attacchi militari. Se, però, questo è vero, è altrettanto vero che i problemi legati alla cybersicurezza sono presenti anche in questo ambito, tanto da aver fatto realizzare all'interno del Ministero degli Affari esteri un ufficio speciale per la cybersicurezza.

Il quadro normativo era, per così dire, obbligato, perché partiva dal recepimento della direttiva dell'Unione europea n. 2555 del 2022, già citata dall'ottimo relatore Nazario Pagano, relativa a misure per un livello comune elevato di cybersicurezza all'interno dell'Unione, che si inserisce in un contesto geopolitico di incremento massiccio degli attacchi indiscriminati a tutti gli Stati dell'Unione. Si tratta, questo va sottolineato, di attacchi tanto nei confronti di privati quanto nei confronti del pubblico.

Emerge chiaramente, quindi, dalla lettura di questo testo, la volontà del Governo di rafforzare ulteriormente il livello della cybersicurezza nazionale, della risposta delle singole amministrazioni, la necessità di potenziare il funzionamento dell'Agenzia, nonché, al tempo stesso, di aumentare le pene minime e massime previste.

Novità importante è anche l'intenzione di modificare la normativa sui contratti pubblici di beni e servizi informatici, laddove dovrà essere svolta un'equa e attenta valutazione dell'elemento quantitativo rispetto a quello qualitativo, per scegliere il miglior rapporto

qualità-prezzo per l'aggiudicazione all'interno delle gare.

A nostro sommesso avviso, bene il forte inasprimento delle pene per i reati informatici, benissimo il coordinamento tra l'Agenzia nazionale e la Direzione nazionale antimafia per la tutela delle infrastrutture critiche. È inutile soffermarsi sull'aumento delle pene, che è stato già brillantemente illustrato dal relatore, ma una parola va spesa per una figura estremamente importante che è stata introdotta, cioè il ravvedimento o pentimento dell'*hacker*. Le pene 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 giudiziaria nella raccolta di elementi di prova - che serviranno poi per i procedimenti futuri - e nel recupero dei proventi dei delitti.

Altro elemento rilevante è l'estensione, e questo va sottolineato, delle intercettazioni per i fatti di criminalità organizzata ai reati informatici rimessi dall'articolo 371-*bis* al coordinamento del procuratore nazionale antimafia. Importante è il coordinamento tra l'Agenzia per la cybersicurezza nazionale e l'autorità giudiziaria per le attività di ripristino, per l'assicurazione delle fonti di prova e l'indispensabile coordinamento col procuratore nazionale antimafia.

C'è, addirittura, la possibilità di differire alcune attività di contrasto, qualora i servizi di sicurezza nazionali lo ritengano necessario ai fini del conseguimento dell'obiettivo principale, che è la tutela della sicurezza dello Stato. È stato istituito l'obbligo di segnalare gli incidenti, da parte di tutte le amministrazioni pubbliche, ed esso è esteso anche alle società *in house*.

Viene creata, all'interno delle amministrazioni, la figura del referente per la cybersicurezza, con l'istituzione di un'apposita struttura, che diventa però il punto di contatto tra quell'amministrazione e l'Agenzia nazionale.

Altro aspetto importante è dato dal fatto che non sia stata dimenticata l'intelligenza artificiale: si prevede infatti la possibilità di promuovere ogni forma, anche di partenariato pubblico, per la valorizzazione dell'intelligenza artificiale come risorsa per il rafforzamento della cibernetica nazionale. L'intelligenza artificiale, che è il tema dominante di queste nostre discussioni, non va demonizzata, ma va usata.

Concludo con una modifica che potrebbe essere foriera di interpretazioni - per così dire - maliziose, sempre per la solita dinamica/dialettica sul rapporto fra politica e magistratura; viceversa, siamo assolutamente favorevoli alla modifica che è stata apportata nel corso dell'esame in sede referente con riferimento alla previsione relativa all'Ispettorato generale presso il Ministero della Giustizia, nell'ambito - e qui è importante dirlo, per evitare polemiche - delle ispezioni ordinarie che vengono periodicamente, - non ricordo se ogni 3 o ogni 5 anni -, compiute all'interno degli uffici giudiziari; chi compie queste ispezioni deve essere chiamato anche a verificare il rispetto delle prescrizioni di sicurezza negli accessi alle banche dati. Mi sembra una cosa che potremmo definire addirittura minimale rispetto all'assetto complessivo della legge.

PRESIDENTE. Non vi sono altri iscritti a parlare e pertanto dichiaro chiusa la discussione sulle linee generali.

(Repliche - A.C. 1717-A)

PRESIDENTE. Prendo atto che il relatore ed il rappresentante del Governo rinunciano alla replica.

Il seguito del dibattito è rinviato ad altra seduta.

Discussione delle mozioni Casu ed altri n. 1-00280 e Iaria ed altri n. 1-00281 concernenti iniziative in materia di trasporto pubblico locale.

PRESIDENTE. L'ordine del giorno reca la

discussione delle mozioni Casu ed altri n. 1-00280 e Iaria ed altri n. 1-00281 concernenti iniziative in materia di trasporto pubblico locale *(Vedi l'allegato A)*.

La ripartizione dei tempi riservati alla discussione è pubblicata nel vigente calendario dei lavori *(Vedi calendario).*

Avverto che in data odierna è stata presentata una nuova formulazione della mozione Casu ed altri n. 1-00280 *(Vedi l'allegato A)*. Il relativo testo è in distribuzione.

(Discussione sulle linee generali)

PRESIDENTE. Dichiaro aperta la discussione sulle linee generali.

È iscritto a parlare il deputato Andrea Casu, che illustrerà anche la sua mozione n. 1-00280 *(Nuova formulazione)*. Ne ha facoltà.

ANDREA CASU (PD-IDP). Grazie, Presidente. Onorevoli colleghi, rappresentante del Governo, oggi noi portiamo all'attenzione dell'Aula della Camera dei deputati, del Parlamento, un tema fondamentale per la vita delle cittadine e dei cittadini italiani. Basta scorrere la rassegna stampa di oggi per leggere dei problemi che ci sono stati: dalla ferrovia Roma Nord - un lunedì da incubo per i pendolari -, ai problemi a Milano per la cancellazione del treno delle 6,53, fino alle questioni dell'Umbria, di cui all'interrogazione della Vicepresidente Ascani, e anche nella giornata di oggi, in tutte le regioni, le periferie e le aree interne: la crisi del trasporto pubblico locale la tocchiamo con mano tutti, ogni giorno. È una crisi che ha ragioni antiche, ma che ha anche questioni assolutamente moderne, che vanno fronteggiate e che non possono più continuare a essere ignorate. Da questo punto di vista, noi abbiamo fatto un grandissimo lavoro in Commissione trasporti. Voglio ringraziare il presidente Deidda e i rappresentanti delle opposizioni, perché è nato tutto da una risoluzione del Partito Democratico in Commissione ma poi ci sono state la risoluzione Raimondo della maggioranza e le risoluzioni Iaria e Ghirra del MoVimento 5 Stelle e di Alleanza Verdi e Sinistra.

Noi ci siamo confrontati con tutto il mondo del trasporto pubblico locale: per alcuni mesi abbiamo fatto il punto e abbiamo cercato di capire qual era lo stato dell'arte e quali potevano essere le soluzioni. Questo confronto c'è stato in Commissione e noi lo portiamo in Aula. Lo facciamo attraverso una mozione che ha alcuni punti molto precisi: nelle premesse ricostruisce e inquadra la questione, ma, nel dispositivo, chiede impegni conseguenti. La prima questione, assolutamente fondamentale, è una questione complessiva, legata alle risorse del Fondo nazionale dei trasporti, perché c'è qualcosa che va detto con grande chiarezza: noi lo chiamiamo trasporto pubblico locale perché ha chiaramente una dimensione locale, ma le grandi scelte che determinano la qualità dei servizi che offriamo ai cittadini sono scelte nazionali, legate anche alla quantità e alla qualità di risorse che mettiamo a disposizione delle regioni e, attraverso le regioni, delle amministrazioni.

Da questo punto di vista, abbiamo avuto cambiamenti, anche molto importanti, intervenuti nella società con la pandemia; abbiamo avuto cambiamenti anche nel mondo del lavoro, nel tipo di trasporti e di mobilità che si verificano nelle nostre città; abbiamo avuto una ripartenza fondamentale del turismo, del *boom* turistico, che ha rimesso in moto anche il traffico verso le nostre città. Abbiamo cambiamenti climatici, che stanno portando a una crescita di costi: pensiamo a tutti problemi che abbiamo avuto la scorsa estate, anche per quanto riguarda come questi cambiamenti climatici hanno influito sulle reti e sui costi. Pensiamo all'aumento dei costi del carburante, pensiamo a tutti questi aumenti, è chiaro che questi aumenti devono impegnare più risorse. C'è una cifra: 1,7 miliardi di euro. È la cifra che le principali agenzie delle imprese hanno chiaramente fotografato, chiesto e ribadito, anche in un recente incontro che si è svolto a Milano in queste ore. Ed è la cifra che consente - lo dicono tutti i sindacati - il rinnovo dei

contratti di quei lavoratori: stiamo parlando di 800 milioni necessari per l'adeguamento del Fondo per quanto riguarda il trasporto pubblico locale, la possibilità dell'adeguamento ai costi inflattivi ed i maggiori costi a cui si va incontro. E poi 900 milioni di euro, che sono indispensabili per il rinnovo dei contratti dei lavoratori. Lavoratori a cui vorrei che, da quest'Aula, venisse mandato trasversalmente un forte messaggio, perché i lavoratori del trasporto pubblico locale e, soprattutto, i lavoratori del *frontline* sono ogni giorno in prima linea. Sono in prima linea per garantire servizi; sono le prime persone a cui si rivolgono i cittadini, anche di fronte ai disservizi e alle difficoltà e, inoltre, sono sempre più oggetto di aggressioni e di minacce: una violenza che si rivolge proprio a loro, che garantiscono un servizio. Ecco, non possono essere lasciati soli. Uno degli impegni che chiediamo al Governo è di garantire la piena operatività di quei protocolli che erano stati siglati e che erano stati avviati nella precedente esperienza di Governo, per fare sì che i lavoratori potessero essere messi nelle condizioni di agire in sicurezza e queste aggressioni potessero essere segnalate e fermate utilizzando le migliori buone pratiche a livello internazionale. Da questo punto di vista, è fondamentale che questi contratti vengano rinnovati. Servono queste risorse; serve questo miliardo e sette. Noi, in sede di bilancio, avevamo presentato, ad esempio, degli emendamenti che sono stati purtroppo bocciati, individuando come una possibile fonte i sussidi ambientalmente dannosi: gli oltre 22 miliardi di sussidi ambientalmente dannosi presenti nel bilancio. Se non è questa la fonte che individua il Governo se ne trovi un'altra, ma è fondamentale che azioniamo la leva del finanziamento nazionale. E questo perché? Perché poi c'è una seconda questione, che è una questione di criteri di attribuzione di questo Fondo. Abbiamo discusso in Commissione, abbiamo idee anche diverse in tal senso, ma siamo tutti d'accordo che il criterio meramente storico non può essere sufficiente. Serve che si tenga conto dei servizi che devono essere garantiti in tutte le città, in tutte le aree urbane ed in tutte le comunità. Non si può avere una divisione fra cittadini di serie A e cittadini di serie B, a seconda che i cittadini nascano nel centro o nelle periferie di una grande città, in un'area interna o in un grande nucleo urbano, perché quella possibilità di avere un'alternativa al mezzo privato per potersi muovere, per poter portare i figli a scuola, per poter andare a lavorare, è una possibilità fondamentale che dobbiamo garantire come pieno diritto di cittadinanza. Ora, da questo punto di vista, una riforma del trasporto pubblico locale e dell'attribuzione di queste risorse è chiaramente una riforma non più rinviabile.

Ci sono alcune ingiustizie: noi abbiamo fatto l'esempio delle città metropolitane e delle difficoltà che affrontano la capitale e Milano, ma anche tutte le altre città metropolitane i cui rappresentanti sono venuti in audizione e ci hanno portato la testimonianza delle loro difficoltà, a cui devono fare fronte. Pensiamo che veramente stiamo parlando di oltre 300 milioni di euro di proprie risorse che mette il comune di Milano, oltre 600 milioni che mette il comune di Roma, e non solo, anche le altre realtà, e poi le difficoltà legate alla copertura dei costi per gli investimenti: penso ai temi delle reti metropolitane, ma non solo.

Penso alla questione di quelle risorse e quegli investimenti garantiti dai nuovi mezzi che, grazie al PNRR, stanno arrivando nelle nostre città. Anche da questo punto di vista, avere un nuovo autobus elettrico significa avere più costi, perché ci sono i costi per il deposito, nuovi costi per le imprese di trasporto e questi costi devono essere coperti. E non si può pensare che l'unica soluzione sia aumentare il costo del biglietto per i cittadini, per due ragioni. La prima è che tutto il mondo va in un'altra direzione: l'idea del biglietto climatico in Germania, l'idea di poter avere il diritto a muoversi e così incentivare le sfide climatiche, incentivare la decarbonizzazione, incentivare, attraverso un trasporto pubblico efficace ed efficiente, un'idea di mobilità sostenibile e sicura per tutte e per tutti; e la seconda è

che poi, a un certo punto, diventa insostenibile comunque. Quanto possiamo far pagare il biglietto? Noi dobbiamo avere una leva che tenga conto del valore che ha il trasporto.

Da questo punto di vista le città metropolitane devono avere alcuni strumenti. Perché chiediamo di mettere mano prima alle risorse e poi ai criteri? Perché, se manteniamo quei 5 miliardi o poco più senza intervenire sulle risorse, rischiamo di avere, con riferimento ai criteri, una guerra tra poveri, un'operazione per cui ci si sposta da una realtà ad un'altra, quando, se esaminiamo il sistema dei trasporti del nostro Paese, vediamo che è un'emergenza nazionale. Servono una riforma organizzativa, una certa attenzione al lavoro. E serve considerare la leva dei trasporti come la leva principale che abbiamo per azionare una direzione di futuro che vada verso una mobilità sostenibile, una mobilità che consenta veramente a tutte le cittadine e a tutti i cittadini di potersi muovere.

Ora, da questo punto di vista, la valutazione politica per cui noi, in queste ore, come Partito Democratico, abbiamo chiesto fortemente di avere questa occasione di confronto sul trasporto pubblico locale è che - è vero - siamo nel pieno di una campagna elettorale, per cui ci possono essere motivazioni, argomentazioni e orientamenti differenti. Ma non possiamo perdere di vista quello che sta accadendo nel Paese. Abbiamo contezza della situazione devastante della sanità. Abbiamo tante paure e preoccupazioni sul tema del lavoro. Non possiamo ignorare anche quello che sta avvenendo sui trasporti. Purtroppo, non sempre si inquadra correttamente quanto siano fondamentali i trasporti; eppure, si tratta di un'attività, forse l'attività a cui dedichiamo più ore del nostro tempo ogni giorno. Ci servono per realizzare tutto il resto.

E quel ritardo nel diritto alla mobilità, nel diritto della cittadinanza a muoversi nelle nostre città lo scontiamo in tutto, perché spesso la nostra percezione dell'assenza di servizi è legata al tempo che ci vuole per arrivarci e non al fatto che ci siano o meno; quindi è legata al traffico, alle ore di traffico che ci separano dal luogo dove possiamo trovare la risposta alla nostra domanda o dalle ore che siamo costretti a trascorrere per poterli raggiungere. E io credo che, da questo punto di vista, abbiamo il dovere di mettere in campo un'azione concreta.

Un ultimo punto importante della mozione: mi auguro veramente che ci possa essere un confronto di merito punto per punto. Ho già letto i contenuti dei primi testi che sono stati presentati. Auspico che ci sia, da parte di tutte le forze politiche, la possibilità di utilizzare questa occasione per fare il punto e dire cosa si pensa del trasporto pubblico locale.

Fatemi aggiungere un ultimo punto. È in corso un'azione molto pericolosa (penso a quello che sta avvenendo con il codice della strada) che va nella direzione di non considerare tutta la mobilità sostenibile come indispensabile. Noi abbiamo bisogno di un'intermodalità che consenta alle persone di muoversi con strumenti diversi che fra loro dialoghino, che garantisca sempre la sicurezza di tutti i mezzi, e che poi vada a colpire proprio quelle amministrazioni e quei poteri che devono avere i sindaci per poter azionare quelle leve, anche territoriali, indispensabili, dalle zone a traffico limitato alla delimitazione delle velocità, fino al tema delle piste ciclabili.

Il codice della strada andava in una direzione sbagliata, noi l'abbiamo contrastato in Parlamento. Lo stiamo contrastando in Senato. Vogliamo leggere positivamente il fatto che il Senato stia prendendo un tempo ulteriore per approfondire, nella speranza che si possano correggere alcuni di questi aspetti e si possa restituire valore ai sindaci, alle amministrazioni e alle autonomie - che vengono considerate tanto importanti e strategiche da questo Governo in altri contesti - anche nel contesto della mobilità e dei trasporti. Però, da questo punto di vista, un accento deve essere molto, molto chiaro, perché, in realtà, è solo azionando pienamente il trasporto pubblico locale che possiamo garantire ai cittadini quel diritto alla mobilità che consentirebbe di vivere in maniera più positiva sia coloro i quali non

vogliono prendere un'auto privata, sia gli stessi automobilisti, i quali si ritroverebbero, potendo avere un'alternativa, strade più sgombre e non occupate dal traffico, spesso soffocante, che fa schizzare, ogni anno di più, le nostre città nelle classifiche internazionali.

È un tema molto importante che si intreccia con altre questioni. Noi dobbiamo far crescere il nostro sistema dei trasporti per poter competere: vi è la grande questione del Sud Italia, del Mezzogiorno d'Italia, che non può restare indietro. E preoccupa anche come l'autonomia differenziata possa forzatamente portarci verso una direzione in cui si fotografa una situazione esistente e poi si peggiora ancora di più.

C'è poi anche la questione - abbiamo detto - del lavoro, della sicurezza sul lavoro, della sicurezza dei lavoratori e delle lavoratrici di fronte alle minacce e alle aggressioni. E c'è anche un'occasione, c'è una questione salariale, legata al fatto che bisogna garantire il lavoro nel trasporto pubblico locale attraverso una forma di contratti - e proprio per questo servono le risorse per il rinnovo subito, ma non solo, servono tanti strumenti - che consenta ai nostri giovani di scegliere di impegnarsi nel trasporto pubblico locale. Se guardiamo l'età media delle persone che lavorano nel trasporto pubblico locale e se guardiamo la fuga, che sta avvenendo, dal trasporto pubblico locale verso altri settori, noi rischiamo veramente, in questo settore fondamentale, strategico, motore dello sviluppo delle nostre città, di andare in una direzione opposta a quella verso cui dovremmo andare.

Come Partito Democratico questo è il nostro impegno, è una delle nostre priorità, insieme alle battaglie che stiamo facendo sulla sanità, sulla scuola, sul lavoro. E questa è l'agenda che noi vorremmo fosse portata avanti in un confronto tra opposizione e maggioranza, in un confronto positivo anche con i soggetti a cui ci si rivolge. E al riguardo, veramente, quello che abbiamo scritto nella mozione, quello che c'è nelle risoluzioni, quello che c'è stato nelle audizioni e ciò che abbiamo fatto lo dicono tutte le imprese del trasporto, lo dicono tutte le amministrazioni, lo dice la Conferenza delle regioni (il presidente Fedriga ha scritto, lo scorso inverno, un documento molto chiaro, indicando molto chiaramente la necessità di queste maggiori risorse a livello nazionale); lo dicono tutti i sindaci delle città metropolitane di destra e di sinistra, lo dicono le realtà insulari e penso alle difficoltà che ci sono nella continuità territoriale. Lo dicono tutti, dobbiamo anche farlo. E credo che una funzione di consapevolezza parlamentare, attraverso queste mozioni, possa essere il primo passo per uscire dal braccio di ferro in cui si indicano le responsabilità di quello che dovrebbe fare qualcun altro e per assumere collettivamente la responsabilità di garantire un servizio di trasporto più adeguato alle nostre città.

Auspichiamo che questo tipo di messaggio possa essere colto e che questo tipo di lavoro possa essere fatto. Noi, sicuramente, continueremo a farlo, non smetteremo e continueremo a batterci per far sì che questa questione venga considerata per quella che è nel dibattito pubblico di tutte le grandi città europee e mondiali e non, purtroppo, come avviene troppo spesso in Italia, come un fanalino di coda.

E qui concludo veramente con una considerazione finale: nessuno pensi che si possa derubricare l'importanza del trasporto pubblico locale o, ancora peggio, scaricare questa responsabilità sulle sole amministrazioni e regioni. Sarebbe un errore da un punto di vista politico, perché tante di queste regioni e di queste amministrazioni ormai sono guidate anche dalla destra.

Quindi, se qualcuno ha immaginato che poter scaricare il fallimento del trasporto pubblico locale sulle spalle delle amministrazioni delle regioni fosse, in qualche modo, un vantaggio politico, evidentemente ha fatto male i propri conti. Infatti, quelle amministrazioni e quelle regioni sono fatte da donne e da uomini che ogni giorno si scontrano con difficoltà crescenti e che non possono più restare da soli. Solo un sistema dei trasporti nel

suo complesso, che azioni tutte le leve, a partire da quella delle risorse, e che metta tutti nelle condizioni di garantire il servizio più efficiente ed efficace, può permettere a quelle persone un miglioramento, che non è merito della singola amministrazione, ma è un merito che viene riconosciuto collettivamente a tutti e, in particolare, a chi oggi ci sta governando. Quindi, portando avanti questa battaglia, nell'interesse dei cittadini, creiamo anche le condizioni per cui ci possa essere una percezione migliore, nel suo complesso, delle istituzioni, anche di chi oggi guida queste istituzioni.

Soprattutto, non dimentichiamo che la situazione sta effettivamente peggiorando. Basta provare a muoversi nelle nostre città. Ieri, tornavo a Roma - e qui veramente concludo -, in treno, con l'alta velocità, parlando con alcuni pendolari, mi rendevo conto - amara consapevolezza - che alcune persone impiegano tre ore per andare da Milano a Roma e poi impiegano lo stesso tempo per andare da Roma o Milano ad altre città o comuni della stessa regione. Noi, questa Italia a due velocità, la dobbiamo fermare. Dobbiamo garantire, anche nel trasporto pubblico locale, quella velocità per godere dei propri diritti che abbiamo garantito con l'alta velocità e con altri strumenti che funzionano. Da questo punto di vista, questa mozione è un primo fondamentale passo.

PRESIDENTE. È iscritto a parlare il deputato Cantone, che illustrerà la mozione Iaria ed altri n. 1-00281, di cui è cofirmatario.

LUCIANO CANTONE (M5S). Grazie, Presidente. Colleghe e colleghi, le infrastrutture della mobilità sostenibile rivestono un ruolo cardine in quanto contribuiscono al benessere dei cittadini e costituiscono il secondo pilastro, dopo il raggiungimento dell'efficienza energetica globale, su cui costruire la transizione ecologica del nostro Paese.

L'obiettivo della neutralità climatica sarà raggiungibile solo attraverso il rinnovamento del sistema dei trasporti in chiave sostenibile. Questo settore oggi è responsabile di circa il 25 per cento delle emissioni di CO2 nel nostro Paese, a causa di un estremo ritardo nel rinnovamento del parco veicoli e del sottoutilizzo del trasporto merci su rotaia.

L'Italia ha una delle flotte di veicoli più vetuste fra i Paesi dell'Europa occidentale. Il parco auto circolante continua a diventare sempre più vecchio e, quindi, sempre più inquinante. Alla fine del 2021, in Italia circolavano sulle strade circa 38,8 milioni di vetture. Se nel 2009 l'età media del parco circolante era di 7,9 anni, progressivamente si è saliti agli attuali 12,5. Molto vecchio è anche il parco circolante degli autobus: l'età media è, infatti, di 12 anni. Il processo di riconversione dei trasporti in Italia è fondamentale al fine di rispettare gli obiettivi del *Green Deal* europeo.

Con la legge di bilancio 2022, è stato istituito il Fondo per la strategia di mobilità sostenibile, che ha una dotazione di 2 miliardi di euro per il periodo 2023-2034, per ridurre le emissioni climalteranti nel settore dei trasporti con diverse azioni, tra cui il rinnovo del parco circolante dei mezzi pubblici. In particolare, il decreto di riparto, nel dettaglio, prevede un miliardo di euro, pari al 50 per cento del Fondo, per interventi sulla mobilità urbana nelle città metropolitane e nei comuni con più di 100.000 abitanti, tra i quali l'acquisto di veicoli elettrici per il trasporto pubblico locale, la realizzazione delle infrastrutture per la ricarica, nonché interventi di pedonalizzazione di aree urbane e per agevolare la mobilità ciclistica. Inoltre, la realizzazione di infrastrutture digitali per la gestione e il monitoraggio dei flussi di carico.

Il trasporto pubblico locale per le regioni a statuto ordinario è finanziato attraverso il Fondo nazionale per il concorso finanziario dello Stato agli oneri del trasporto pubblico locale, anche ferroviario, istituito dalla legge n. 228 del 2012. Gli stanziamenti del Fondo si trovano nel bilancio dello Stato sul capitolo n. 1315 dello stato di previsione di spesa del Ministero delle Infrastrutture e dei trasporti. Come è noto, la suddivisione tra le regioni, in deroga alle

più recenti disposizioni normative, si basa sul principio della spesa storica, che ormai non rappresenta più le variabili che rilevano per il servizio agli utenti: territorio servito, chilometri coperti, abitanti, flussi di trasporto reali, qualità del servizio e altro.

Risulta emblematico sotto questo profilo il caso di Roma capitale. L'ATAC, che da sola rappresenta il 16 per cento della media nazionale per numero di passeggeri trasportati ante-COVID e per il 7 per cento dell'offerta nazionale in termini di produzione chilometrica, ai sensi del succitato riparto, riceve dalla regione Lazio la quota parte. Lo Stato non finanzia direttamente il trasporto pubblico locale di Roma capitale - eccetto le ferrovie concesse - con lo strumento del Fondo. Gli unici trasferimenti ad oggi esistenti, pari a circa 250 milioni di euro annui, sono assolutamente insufficienti e destinati a variare senza tenere conto del reale bisogno della capitale.

Al fine di agevolare l'uso generalizzato dei mezzi pubblici è stato approntato e poi rifinanziato negli anni il cosiddetto *bonus* trasporti, volto a sostenere l'acquisto degli abbonamenti da parte dei cittadini. Si tratta di una misura fortemente apprezzata, perché, dapprima, ha sostenuto lo *shift* modale e, successivamente, in modo semplice e diretto, i bilanci familiari.

È fondamentale avere un adeguato sistema di trasporto pubblico locale che risponda alle esigenze di uno sviluppo sostenibile sotto il profilo sociale, economico e ambientale. Non è accettabile, infatti, che il diritto alla mobilità non sia garantito, specie nei contesti urbani più problematici.

Il rapporto Pendolaria 2024 fotografa una situazione del trasporto ferroviario in Italia dove persistono differenze marcate sulla qualità e la quantità del servizio, in particolare tra Nord e Sud e tra linee principali e secondarie, dove le prospettive richiedono un impegno maggiore. Un dato che merita una certa attenzione riguarda proprio le ferrovie regionali di Calabria e Sicilia, che hanno una flotta di treni locali rispettivamente dell'84 per cento e del 67 per cento più vecchia di 15 anni. Inoltre, il contratto collettivo nazionale di lavoro autoferrotranvieri e internavigatori 2024 -2027 non è stato ancora rinnovato e sottoscritto e, pertanto, da marzo 2024 assistiamo ad un inasprimento delle vertenze sindacali. Le motivazioni del settore riguardano la necessità di un aumento salariale, la riduzione dell'orario di lavoro da 39 a 35 ore a settimana, parità di salario con riduzione del periodo di guida per gli autisti, aumento delle tutele in tema di sicurezza e di salute sul lavoro.

In questo contesto, come MoVimento 5 Stelle abbiamo chiesto, con questa mozione, un impegno al Governo: a sostenere le iniziative di competenza volte a velocizzare la sostituzione dei mezzi più vetusti con quelli ambientalmente più sostenibili, con particolare riguardo alle aree metropolitane, aumentando gli investimenti per la propulsione elettrica, ad idrogeno verde, considerando anche l'ipotesi di mezzi ibridi elettrico/metano; ad adottare iniziative di competenza volte a definire necessarie linee guida per la redazione e la valutazione di progetti concernenti l'utilizzazione di strutture ferroviarie di carattere locale, anche attraverso la realizzazione di nuove infrastrutture a esse collegate per il transito di tram e di veicoli leggeri su rotaia, secondo quanto previsto dalla direttiva (UE) 2016/797; ad adottare iniziative di competenza volte a reperire risorse economiche necessarie all'adeguamento del contratto collettivo nazionale del trasporto pubblico locale e a sostenere le richieste dei lavoratori, con particolare riguardo alle riduzione dell'orario di lavoro e alla parità di salario; a sostenere il diritto alla mobilità dei cittadini attraverso un aumento del Fondo nazionale per il concorso finanziario dello Stato agli oneri del trasporto pubblico locale, prevedendo nell'ambito del riparto dello stesso forme di perequazione territoriale, evitando, per quanto di competenza, che l'assetto regionale impatti negativamente sull'uniforme garanzia dei servizi locali di trasporto pubblico e prevedendo, nel caso di Roma Capitale, l'assegnazione diretta del fondo,

che consenta di attribuire risorse aggiuntive al riparto stabilito per la regione Lazio; ad adottare iniziative di competenza necessarie per scongiurare gli imminenti aumenti del costo della bigliettazione per il trasporto pubblico locale con particolare riguardo a quello urbano; a chiarire la preoccupante situazione relativa al *dossier* riguardante il ponte sullo Stretto di Messina, posto che, nelle more dell'iter di approvazione della legge di bilancio per l'anno 2024, sono stati distratti 2,3 miliardi di euro dal Fondo per lo sviluppo e coesione per Calabria e Sicilia verso questa grande opera; al fine di non mettere in crisi i servizi pubblici locali di Calabria e Sicilia, tra cui il trasporto pubblico locale, a prevedere, rifinanziamento statale di fondi FSC destinati al ponte sullo Stretto; a prevedere iniziative di competenza, anche di carattere normativo, volte ad aumentare la deducibilità per l'acquisto e il noleggio di veicoli a zero emissioni sia per le imprese che per i lavoratori al fine di supportare la transizione verso la mobilità sostenibile, anche modificando l'articolo 51, comma 2, del testo unico delle imposte sui redditi, per includere l'acquisto di energia per la ricarica elettrica e l'installazione di *wallbox* come spese deducibili per i lavoratori dipendenti.

Chiediamo, inoltre, al Governo di adottare iniziative per l'accesso agli incentivi per i veicoli a zero emissioni senza la necessità di rottamare un veicolo più vecchio e il supporto al noleggio di tali veicoli e volte ad esentare dal pedaggio autostradale i veicoli elettrici; a rendere le stazioni ferroviarie *hub* della mobilità condivisa ed elettrica e ad utilizzare i fondi del Piano strategico nazionale di mobilità sostenibile e del PNRR anche per il noleggio di veicoli elettrici, oltre che a ridurre gli oneri di sistema per le aziende di trasporto pubblico locale.

PRESIDENZA DELLA VICEPRESIDENTE ANNA ASCANI *(ore 18,07)*

LUCIANO CANTONE (M5S). Chiediamo inoltre di adottare ogni iniziativa di competenza, anche di carattere normativo, finalizzata a promuovere l'impiego dei monopattini, incentivando e semplificando l'uso dei mezzi di mobilità dolce e sostenibile, ed evitando ogni intervento che risulti vessatorio per gli utilizzatori.

Inoltre, l'impegno che chiediamo è anche finalizzato a velocizzare il progetto "*Mobility as service for Italy*" del Piano nazionale di ripresa e resilienza che punta ad arrivare a una completa digitalizzazione e intermodalità del trasporto pubblico locale su scala nazionale; ad adottare, infine, le opportune iniziative per introdurre una data limite di utilizzo esclusivo di imbarcazioni elettriche sui fiumi e laghi nazionali per il finanziamento del *retrofit* delle imbarcazioni termiche e l'allocazione di fondi per il trasporto pubblico navale. Chiudiamo questa mozione chiedendo di adottare iniziative per quanto riguarda la realizzazione di vertiporti, per la decarbonizzazione del trasporto locale e la promozione delle attività sperimentali in questo settore.

PRESIDENTE. È iscritto a parlare il deputato Amich. Ne ha facoltà.

ENZO AMICH (FDI). Grazie, Presidente. Vice Ministro Gava, onorevoli colleghi, la mozione di maggioranza che ci apprestiamo a discutere vuole rispondere alle critiche formalizzate dall'opposizione in un documento analogo che esamineremo contestualmente al nostro. La convinzione dalla quale partiamo è che la garanzia di un trasporto pubblico locale adeguato su tutto il territorio è, non solo un diritto sancito dall'articolo 16 della Carta costituzionale, ma anche un fondamento di coesione economica e sociale. Un servizio di trasporto pubblico adeguato su tutto il territorio è, quindi, anche tra i fondamenti dell'uguaglianza sostanziale di tutti i cittadini, sia sul piano sociale che su quello economico.

Nel corso del tempo, il diritto alla mobilità ha conosciuto diverse declinazioni sul piano legislativo. Prima, nel 1997, il settore del trasporto pubblico locale veniva finanziato con

trasferimenti statali tramite il Fondo nazionale per i trasporti, sia con contributi di esercizio sia con contributi agli investimenti. Con il decreto legislativo n. 422 del 1997, lo Stato ha trasferito la competenza in materia di trasporto pubblico locale alle regioni. Questa riforma, confermata poi anche dalla Corte costituzionale con sentenza n. 222 del 2005, ha introdotto alcune innovazioni: distinzione tra funzioni di regolazione e funzione di gestione operativa dei servizi; trasformazione obbligatoria delle aziende speciali in società di capitali; introduzione del contratto di servizi come strumento per regolare il rapporto tra ente locale e gestore del servizio di trasporto locale e una graduale copertura dei costi del servizio mediante tariffa, con un progressivo incremento rapporti-ricavi e traffico-costi fino al 35 per cento.

Importanti innovazioni si sono avute anche sul meccanismo di finanziamento al trasporto pubblico locale. Il Fondo nazionale per il trasporto pubblico locale, istituito dalla legge stabilità nel 2013, con una consistente dotazione finanziaria annuale e ripartito tra le regioni con le modalità e le percentuali stabilite dal testo di legge stesso, è stato riformato con il decreto-legge n. 50 del 2017. In particolare, è stata stabilizzata in via normativa l'entità del Fondo e sono state introdotte innovazioni relativamente alla sua gestione. In verità, tra le varie disposizioni questo decreto ha previsto una riforma dei criteri di attribuzione del Fondo, che si sarebbe dovuta applicare a decorrere dal 2020, ma la sua applicazione è stata più volte rinviata.

Con la legge delega sul federalismo fiscale, la legge n. 42 del 2009, si è introdotto per il settore del trasporto pubblico regionale una sorta di criterio misto di finanziamento che tiene conto, oltre che dei costi standard, anche della fornitura di un livello adeguato del servizio su tutto il territorio nazionale. Con questo testo si puntava a realizzare una forma di federalismo che avrebbe portato al superamento del criterio della spesa storica, con i livelli essenziali delle prestazioni (LEP) validi per tutto il territorio nazionale, finanziati in base alla previsione del fabbisogno standard. Ciò non è mai avvenuto purtroppo, come dimostrato dalle disparità che si evidenziano ogni qual volta si confrontano comuni italiani con lo stesso numero di abitanti. Siamo convinti che, per non aver applicato i LEP, esso abbia impedito, di fatto, di offrire servizi efficienti ai propri cittadini.

Con l'emergere della crisi pandemica del COVID-19, sono state introdotte numerose disposizioni a sostegno del settore del trasporto pubblico locale, tanto che si potrebbe a buon diritto parlare di una nuova dimensione della mobilità come riflesso dell'emergenza sanitaria. Poniamoci però una domanda: quali sono i tratti che meglio descrivono il nostro sistema di trasporto pubblico locale e che ne descrivono e motivano anche le criticità?

Va detto, innanzitutto, che l'accessibilità sistematica al servizio di trasporto pubblico locale automobilistico è profondamente diversa nelle aree a minore domanda, in quelle periferiche e nei borghi antichi. Quest'ultimi manifestano, infatti, rispetto ai centri urbani, maggiori criticità legate all'abbandono e all'isolamento e mostrano un'eccessiva frammentazione amministrativa e produttiva. Va da sé che, in questi ambiti territoriali, l'accesso al trasporto pubblico debba essere garantito a tutti e, soprattutto, alle persone con mobilità ridotta. In questa materia, l'Unione europea si è espressa con una proposta di direttiva per l'adozione dell'Atto europeo sull'accessibilità e ha inserito nella sua agenda il tema delle problematiche legate all'accessibilità, da intendersi, in questo caso, in un'accezione molto ampia, a comprendere prodotti, servizi, infrastrutture e tutto quanto serva per semplificare gli accessi e gli usi da parte di persone con disabilità e non solo. In Italia, secondo una stima del Censis, oltre 4 milioni sono le persone portatrici di disabilità, con un *trend* stimato in crescita stimato fino a 6,5 milioni di persone nel 2040.

Sempre riguardo ai procedimenti comunitari in materia di mobilità, vale la pena in questa sede ricordare che l'Unione europea, con

regolamento n. 1370 del 2007 del Parlamento europeo e del Consiglio, ha individuato i cosiddetti servizi minimi come quegli obblighi di servizio pubblico intesi a garantire frequenza, qualità, regolarità per il trasporto sicuro a costi ragionevoli e di elevata qualità.

Anche il turismo svolge un ruolo strategico, direi fondamentale, nello sviluppo economico di tutte le nostre regioni e il trasporto pubblico ricopre da sempre una funzione essenziale nelle dinamiche economiche e turistiche, aspetti che costituiscono la struttura portante del sistema territorio-turismo-trasporti per sostenere flussi di mobilità che oggi non possono più considerarsi eccezionali, ma sistematici. Purtroppo, con il trascorrere del tempo, la ridotta perequazione dei trasferimenti si è difatti tradotta in un'affannosa copertura delle spese correnti legate alla gestione dei contratti di servizio a scapito degli investimenti, ossia a scapito della ricerca di standard quantitativi e qualitativi del servizio di TPL in linea con le esigenze della mobilità urbana e di chi utilizza il trasporto pubblico per studio, lavoro o tempo libero.

Queste importanti premesse sono alla base dell'analisi che ha portato i firmatari di questa mozione a introdurre il concetto dei livelli essenziali di trasporto (LET), vale a dire quel complesso di prestazioni di servizi che l'amministrazione pubblica deve fornire a tutti i cittadini se veramente si vuole garantire il rispetto di quel diritto che abbiamo citato all'inizio, più volte riscontrato anche nella Costituzione e, spesso, purtroppo, trascurato in molte aree del territorio nazionale in ambito sia urbano che extraurbano.

I livelli essenziali di trasporto devono rispondere a finalità ben definite ed essere solidamente basati su un concetto di trasporto pubblico concepito a condizioni accessibili per tutti, integrativo alla mobilità privata, anche con forme diverse dalle soluzioni tradizionali, che prevedono collegamenti con bus tradizionali, che mediamente viaggiano con fattore di carico che non supera il 50 per cento di capienza, e autobus che non circolano vuoti in determinate ore della giornata in corrispondenza di specifici territori. Il LET può rappresentare a buon diritto la base per la riorganizzazione dell'ex Fondo nazionale trasporti e la conseguente ripartizione tra regioni e province autonome, ricorrendo a specifici indicatori che tengano conto delle caratteristiche del territorio e dell'economia, della demografia, della domanda di mobilità, oltre che dei parametri caratteristici dell'offerta di trasporto e, in minima parte, stiamo parlando del 10 per cento della spesa storica.

È necessaria una legge di riforma del TPL, con l'obiettivo di disegnare modelli di intervento in grado di connettere i territori nei luoghi più disagiati, suggerendo soluzioni intelligenti attraverso un alto livello di tecnologia *hi-tech*, incentivando, al contempo, l'utilizzo di applicazioni per integrare diverse forme di trasporto, che dovranno essere *green* e sostenibili, a partire dal soddisfacimento degli spostamenti delle persone con disabilità.

Vengo ora ai punti sui quali la mozione di maggioranza intende impegnare il Governo. La IX Commissione (Trasporti, poste e telecomunicazioni) della Camera dei deputati, presieduta dall'onorevole Deidda, di cui sono componente, in data 13 aprile 2024, ha approvato, tra le altre, la risoluzione n. 8-00042, sottoscritta dai firmatari del presente atto, che poneva queste tematiche al centro dell'agenda del Governo e della maggioranza, nella quale erano contenuti gli impegni necessari per affrontare in modo efficace le problematiche evidenziate. Essa impegna il Governo: ad adottare iniziative normative volte a definire una nuova disciplina di riforma del TPL, di supporto agli indirizzi regionali; a valutare l'opportunità di programmare, per quanto di competenza, una serie di iniziative per la definizione di un nuovo strumento essenziale per "disegnare" modelli di intervento a supporto delle regioni, delle città metropolitane e dei comuni con più di 15.000 abitanti sulla base di un sistema innovativo di pianificazione del sistema, che citavamo prima, territorio-trasporti -turismo; ad adottare le opportune iniziative, per quanto di competenza, volte ad assicurare

maggiori connessioni per la mobilità degli utenti, in particolare anziani, pendolari, persone con disabilità, nonché per le aree più isolate e svantaggiate dal punto di vista geografico.

Impegna a promuovere uno studio del settore finalizzato alla definizione del concetto di livelli essenziali di trasporto, ovvero prestazioni e servizi che l'amministrazione pubblica è tenuta a fornire con tutti i cittadini in ragione del rispetto di quel diritto alla mobilità richiamato più volte nella Costituzione italiana sulla base dei livelli essenziali di prestazione; ad adottare iniziative di competenza volte ad introdurre, ai fini del riparto del nuovo Fondo TPL, il concetto innovativo dei livelli essenziali di trasporto quale sintesi delle disposizioni del decreto-legge n. 36 del 2023 e del decreto legislativo n. 201 del 2022, come esposto in premessa, nonché un nuovo modello di ripartizione della spesa pubblica che consideri specifici indicatori in tema di territorio, demografia, economia, mobilità, offerta di trasporto e, in minima parte, spesa storica; ad adottare, compatibilmente con i vincoli di finanza pubblica e nel rispetto delle norme europee sugli aiuti di Stato, le opportune iniziative volte ad agevolare ulteriormente gli investimenti delle aziende di trasporto pubblico locale, in un rinnovo del parco circolante che tenga conto delle diverse tecnologie, combustibili e dei mezzi al fine di garantire più efficienza nella circolazione e una riduzione delle emissioni inquinanti.

Il trasporto pubblico locale necessita di una profonda rivisitazione nella sua organizzazione a livello centrale, e quindi, a cascata, a livello regionale. Le condizioni ormai ci sono tutte, così come i presupposti per una nuova regolazione. Ritengo che siano temi sui quali, al di là della dialettica che esiste tra maggioranza e opposizione, si debba fare realmente squadra, perché ne va dell'interesse del Paese. Spero comunque che dal dibattito scaturito da queste mozioni, che riprende in parte il dibattito innescato in passato da documenti di contenuto analogo che sono stati discussi in quest'Aula, emerga pacificamente la necessità di porre mano a una serie di riforme del TPL i cui contenuti sono stati delineati per quanto attiene alle soluzioni da noi proposte.

PRESIDENTE. Non essendovi altri iscritti a parlare, dichiaro chiusa la discussione sulle linee generali.

Il Governo si riserva di intervenire successivamente. Il seguito della discussione è rinviato ad altra seduta.

Discussione della proposta di legge: Dori e D'Orso; Pittalis ed altri; Maschio ed altri: Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e del cyberbullismo (Approvata, in un testo unificato, dalla Camera e modificata dal Senato) (A.C. 536-891-910 -B).

PRESIDENTE. L'ordine del giorno reca la discussione della proposta di legge, già approvata, in un testo unificato, dalla Camera e modificata dal Senato, nn. 536-891-910-B: Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e del cyberbullismo.

Avverto che lo schema recante la ripartizione dei tempi è pubblicato nell'*allegato A* al resoconto stenografico della seduta del 10 maggio 2024 *(Vedi l'allegato A della seduta del 10 maggio 2024)*.

(Discussione sulle linee generali - A.C. 536-B)

PRESIDENTE. Dichiaro aperta la discussione sulle linee generali.

I presidenti dei gruppi parlamentari Partito Democratico-Italia Democratica e Progressista e MoVimento 5 Stelle ne hanno chiesto l'ampliamento.

Le Commissioni II (Giustizia) e XII (Affari sociali) si intendono autorizzate a riferire oralmente.

Ha facoltà di intervenire il relatore per la Commissione giustizia, deputato Dori.

DEVIS DORI*, Relatore per la II Commissione.* Grazie, Presidente. Siamo finalmente giunti alle battute finali di questo articolato percorso legislativo volto alla prevenzione e al contrasto del bullismo e del cyberbullismo. Dopo l'approvazione all'unanimità, in prima lettura, alla Camera, il 6 settembre del 2023, è arrivata poi l'approvazione con alcune modifiche al Senato, sempre all'unanimità, il 22 febbraio scorso, e ora ci apprestiamo a darne approvazione definitiva.

Una cosa che ho ben appreso in questi anni di attività parlamentare è che nessun risultato è mai scontato, nessun provvedimento arriva a meta per mera inerzia. Se oggi, quindi, siamo a un passo da questa approvazione entro la prima metà della legislatura, è perché tutti, davvero tutti, hanno remato dalla stessa parte. Tutti abbiamo sempre avuto il medesimo obiettivo, ma non partivamo esattamente dalle stesse premesse sugli strumenti da adottare. Ma l'obiettivo comune ci ha consentito di fare tutti insieme dei passi, piccoli passi indietro, singolarmente, per poter fare insieme un passo in avanti decisivo. Su questo tema si può correttamente parlare di percorso parlamentare sia perché si è svolto interamente in ambito parlamentare sia perché il disegno di legge in esame ha le sue prime radici nella scorsa legislatura, in quella proposta di legge, a mia prima firma, che era stata depositata nel gennaio 2019 assieme alla collega Valentina D'Orso, poi approvata alla Camera il 29 gennaio 2020, pochi giorni prima dello scoppio della pandemia. Un iter che poi, però, si bloccò al Senato, ma che, grazie alla dichiarazione d'urgenza votata all'unanimità qui, nel febbraio 2023, ci ha permesso di iniziarne l'iter immediatamente, dall'inizio di questa legislatura.

Rapidamente, prima di alcune considerazioni generali, analizzo alcuni aspetti più rilevanti del disegno di legge. L'articolo 1, anzitutto, estende e amplia il perimetro di applicazione della legge n. 71 del 2017, che attualmente si occupa di prevenzione e contrasto del solo cyberbullismo, alla prevenzione e al contrasto anche di quel bullismo che possiamo definire *offline*, ponendo quindi l'accento soprattutto sulle azioni di carattere preventivo. Interviene, inoltre, l'articolo 1, sempre sulla legge n. 71, prevedendo che ogni istituto scolastico, nell'ambito della propria autonomia, adotti un codice interno per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo e istituisca un tavolo permanente di monitoraggio, del quale fanno parte rappresentanti degli studenti, degli insegnanti, delle famiglie ed esperti del settore.

L'articolo 2, invece, compie un vero e proprio *restyling* all'articolo 25 del regio decreto-legge n. 1404 del 1934. Si tratta di uno strumento che, se utilizzato opportunamente dai tribunali per i minorenni, può assolutamente avere grande efficacia nei casi di bullismo. Infatti, abbiamo introdotto un nuovo strumento, che abbiamo chiamato progetto di intervento educativo, attivabile non solo in caso di bullismo, ma per tutti quei casi di condotte aggressive, anche in gruppo, così come singolarmente, anche per via telematica, ma non necessariamente, nei confronti di persone, animali o cose. L'obiettivo è intervenire sulle condotte aggressive agite dai minorenni, anche infraquattordicenni, perché queste sono misure amministrative applicabili anche ai minorenni non imputabili. Qui, infatti, non si tratta di sanzioni penali, ma di misure amministrative, e quindi questo significa che potranno essere attenzionati quei fenomeni e quei comportamenti indice di forte disagio sociale o di pericolosità sociale. Inoltre, ci sono alcuni aspetti rilevanti in questo nuovo articolo 25, cioè il fatto che si preveda l'ascolto preventivo del minorenne e anche la possibilità, mai prevista finora, di essere anche assistiti da un difensore nell'ambito di un procedimento amministrativo.

L'articolo 3 contiene una delega al Governo, da esercitarsi entro 12 mesi dalla data di entrata in vigore del provvedimento, e prevede il potenziamento del servizio per l'assistenza psicologica o giuridica delle vittime di atti

di bullismo attraverso il numero pubblico Emergenza infanzia 114, dotato anche di un servizio di geolocalizzazione e di un servizio di messaggistica istantanea accessibile gratuitamente e attivo nell'arco delle 24 ore, e nei casi più gravi informando prontamente l'organo di Polizia.

Poi prevediamo, sempre in questa delega al Governo, lo svolgimento di rilevazioni statistiche, almeno biennali, da parte dell'Istat. Nei contratti degli utenti con i fornitori di servizi di comunicazione e informazione offerti mediante le reti di comunicazione elettronica il richiamo delle disposizioni di cui all'articolo 2048 del codice civile in materia di responsabilità dei genitori per i danni cagionati dai figli minori in conseguenza di atti illeciti posti in essere attraverso l'uso della rete.

E poi la promozione di periodiche campagne informative di prevenzione e di sensibilizzazione sull'uso consapevole della rete Internet, sui suoi rischi, e quindi campagne informative da parte della Presidenza del Consiglio dei ministri.

Nell'articolo 4 istituiamo il 20 gennaio come Giornata del rispetto quale momento di approfondimento e sensibilizzazione delle tematiche del rispetto degli altri, del contrasto di ogni forma di discriminazione. Ed è stata scelta come data proprio il 20 gennaio perché il 20 gennaio 1999 nasceva Willy Monteiro Duarte, ucciso durante un pestaggio, il 6 settembre 2020, a Colleferro, nel tentativo di difendere un amico in difficoltà. Willy, quindi, può essere definito un vero e proprio eroe del nostro tempo, difendendo un proprio amico dalla prevaricazione, quella prevaricazione di cui il bullismo si alimenta. Pertanto la figura di Willy Monteiro Duarte deve entrare nelle scuole attraverso questa Giornata del rispetto come antidoto al bullismo.

Infine, l'articolo 5 prevede anche modifiche al cosiddetto statuto delle studentesse e degli studenti affinché il patto educativo di corresponsabilità possa prevedere due nuovi specifici impegni.

Anzitutto l'impegno delle famiglie a partecipare alle attività di formazione che la scuola e i docenti intendono organizzare a favore degli studenti e delle loro famiglie, con particolare riferimento all'uso della rete Internet e delle comunità virtuali, e poi il reciproco impegno della scuola e delle famiglie a collaborare per agevolare l'emersione di episodi riconducibili ai fenomeni del bullismo e del cyberbullismo e di situazioni di uso e abuso di alcol o di sostanze stupefacenti o di forme di dipendenza dei quali i genitori o gli operatori scolastici dovessero avere notizia.

In questo provvedimento ritroviamo tutti gli strumenti efficaci attivabili contro il bullismo, che sono sostanzialmente 5: la prevenzione, il contrasto, l'emersione, il monitoraggio e la sensibilizzazione.

Certamente, il primo strumento deve essere sempre la prevenzione, coinvolgendo ragazzi minorenni, ma, come sappiamo, qualcosa potrebbe sempre sfuggire alle maglie della prevenzione; quindi, la vera sfida è l'equilibrio tra prevenzione e contrasto, e qui lo troviamo proprio all'interno dell'articolo 25, così come riformato da questa proposta di legge, quindi, con una sanzione di natura rieducativa in ambito amministrativo e non penalistico.

Oltre alla prevenzione e al contrasto dobbiamo, però, sempre di più, dare centralità a un terzo elemento: l'emersione degli episodi di bullismo. Occorre, cioè, fare emergere questi episodi tempestivamente, prima che sfocino in qualcosa di più grave. Sappiamo, infatti, che il bullismo, soprattutto quello *offline*, passa sotto traccia e si nasconde tra i sorrisi di derisione, tra le offese sussurrate, tra le azioni di isolamento dal gruppo. Quindi, la vera sfida è individuare quegli strumenti che consentono l'emersione tempestiva di questi episodi, con il coinvolgimento di tutti i soggetti che, a vario titolo, gravitano attorno a quel dramma.

A questi elementi - prevenzione, contrasto ed emersione - ne aggiungo un altro altrettanto importante: il monitoraggio del fenomeno. È, infatti, fondamentale avere una fotografia esatta di questo fenomeno per poi poter pensare di intervenire efficacemente.

Dobbiamo aggiungere anche l'elemento della sensibilizzazione, cioè, occorre attuare delle efficaci iniziative comunicative, pubblicità progresso, anche con il coinvolgimento di personalità del mondo dello sport, della musica, dello spettacolo, che risultano per tanti ragazzi dei punti di riferimento e che, quindi, da lì, possono lanciare anche dei messaggi positivi.

Tutto ciò verso una consapevolezza piena di che cosa sia il bullismo. Solo quando si dà il nome giusto a ogni cosa è possibile intervenire efficacemente e devo ammettere che, oggi, i nostri ragazzi, i nostri studenti hanno un livello di consapevolezza maggiore sul bullismo rispetto alle precedenti generazioni che, invece, ancora, purtroppo, spesso lo riconducono nell'ambito dello scherzo, della ragazzata o, peggio ancora, del "l'abbiamo fatto tutti". No, non è vero: il bullismo è violenza e, come tale, va gestito e contrastato.

Per quanto con l'approvazione di questa proposta di legge l'Italia si doti di una delle legislazioni antibullismo più avanzate in Europa, in ogni caso, non possiamo pensare che una legge sia una sorta di formula magica con la quale si possa spazzare via o risolvere in un sol colpo un problema sociale drammatico come il bullismo.

Le norme, invece, hanno il compito arduo di identificare un nucleo essenziale di strumenti giuridici capaci di adattarsi a contesti sociali differenti. Quindi, come non si poteva ritenere concluso il lavoro con la legge n. 71 del 2017 - e basta vedere i dati: dal 2017 ad oggi i dati sul bullismo sono in continua crescita - probabilmente, anche dopo questa proposta di legge, il percorso non sarà concluso.

Il contenuto di una legge o di una proposta di legge va concepito come un contributo per raggiungere quel risultato voluto, per agevolarlo, indirizzarlo, ma serve un percorso, un processo culturale di durata indefinita e, in questo senso, la proposta di legge certamente ha un ruolo fondamentale, anche nell'indurre, nel creare una consapevolezza maggiore di un dramma sociale.

Ecco, questa proposta di legge che, presto, diventerà, quindi, legge dello Stato ci lascia in eredità un ulteriore impegno, un dovere verso i nostri giovani. Noi, ora, abbiamo studiato gli strumenti per prevenire e contrastare il bullismo, ma dovremo compiere un ulteriore *step*: ragionare anche sugli effetti psicofisici causati dal bullismo. Quali sono gli effetti del bullismo sulla vittima, quali le ferite e come si rimarginano - se si rimarginano - quelle ferite? Allora, dovremo indagare, ad esempio, il rapporto fra il bullismo e i disturbi del comportamento alimentare; e c'è, da questo punto di vista, un interessante approfondimento sul sito di Animenta, un'associazione no profit per i disturbi alimentari, sulla correlazione fra bullismo e disturbi del comportamento alimentare. Il bullismo, causando una sofferenza psicologica profonda, può contribuire allo sviluppo di una patologia alimentare, in quanto essa è espressione di un dolore ed è meccanismo di difesa dallo stesso.

Il bullismo, quindi, pur non essendo l'unico fattore, può determinare e, certamente, contribuire in modo significativo a sviluppare un disturbo alimentare. Secondo uno studio, ben il 65 per cento delle persone con disturbi alimentari afferma che il bullismo ha contribuito alla propria condizione. L'insorgenza di patologie alimentari è particolarmente frequente nei bambini e negli adolescenti che sono stati vittime di bullismo per il loro corpo e la loro forma fisica. Benché qualsiasi disturbo alimentare possa essere causato o impattato dal bullismo, l'anoressia è stata riconosciuta come il disturbo che più spesso ne consegue. In una situazione in cui un individuo subisce bullismo per qualcosa che non può controllare, l'anoressia può insorgere come manifestazione del tentativo di compensare tale mancanza di controllo.

Quindi, proteggere le vittime significa anche proteggere i bulli stessi dal disagio che manifestano con i propri atti violenti. Chiunque, potenzialmente, può provocare dolore agli altri e riconoscerlo è il primo passo per sapersi

fermare in tempo utile. Spesso si ritiene che il bullo sia privo di empatia, in tanti casi, invece, è proprio l'opposto, perché l'empatia, cioè la capacità di mettersi nei panni degli altri, può anche essere usata male, consentendo di individuare i punti deboli altrui e utilizzarli per indurre specifica sofferenza. Noi, invece, dobbiamo creare le condizioni per sviluppare un'empatia costruttiva, sintetizzabile anche nella cosiddetta regola aurea del non fare agli altri ciò che non vorresti fosse fatto a te stesso.

Concludo con l'auspicio che l'articolo 3, che contiene la delega al Governo, possa avere una piena attuazione rapida da parte, appunto, del Governo, addirittura anche con tempi più ristretti rispetto ai 12 mesi previsti. Io credo che ce l'abbiamo messa tutta e che l'approvazione all'unanimità lanci un segnale positivo al Paese di unità della politica nella lotta a questo odiosissimo dramma.

Rammento che questo lavoro non l'abbiamo fatto per noi, ma per i nostri figli, i nostri nipoti e per tutti gli Andrea Spezzacatena che, a oltre 11 anni dal suicidio, il 20 novembre 2012, ci ricorda che si può essere emarginati e umiliati anche solo per il colore dei propri pantaloni. Se con questo lavoro, quindi, saremo riusciti a salvare anche solo un ragazzo o una ragazza, allora, vorrà dire che avremo fatto il nostro dovere.

PRESIDENTE. Ha facoltà di intervenire la rappresentante del Governo, che vi rinunzia.

È iscritto a parlare il deputato Paolo Pulciani. Ne ha facoltà.

PAOLO PULCIANI (FDI). Presidente, onorevoli colleghi, Vice Ministro Gava, oggi, approda in Aula per la discussione generale la proposta di legge in materia di prevenzione e contrasto al bullismo e al cyberbullismo, già approvata dalla Camera dei deputati in un testo unificato e, poi, modificata dal Senato in data 22 febbraio 2024 e che, come sappiamo, reca disposizioni volte a prevenire e contrastare i fenomeni del bullismo e del cyberbullismo. L'esame odierno, quindi, e poi quello che verrà, in Aula, verteranno soltanto sulle modificazioni che sono state apportate al Senato e che andrò poi, di qui a poco, ad affrontare e ad analizzare.

Com'è noto, questa normativa, che il relatore ha sufficientemente descritto, ha l'obiettivo di contrastare e, per quanto possibile, di prevenire tutti quegli atti - anche prodromici - riferiti al bullismo e di farlo in sinergia con le scuole, gli enti locali e le famiglie. Tutto ciò estendendo il perimetro di applicazione della legge n. 71 del 2017, che è stata poc'anzi richiamata, che era una buona legge, ma sicuramente meritevole di aggiornamento rispetto alle nuove emergenze che abbiamo verificato, privilegiando azioni di carattere formativo ed educativo, assicurando l'attuazione degli interventi senza distinzione di età, nell'ambito delle istituzioni scolastiche, delle organizzazioni sportive e in quelle del Terzo settore.

La norma ha anche il pregio, come già ampiamente discusso in quest'Aula, di estendere la disciplina di contrasto del cyberbullismo anche con una nozione più estesa del bullismo *tout court*, dando a questo una definizione più esatta e precisa. Infatti, è importante, a volte, anche la definizione degli stessi atteggiamenti che possono provocare danni o essere in qualche modo contro qualcuno, provocando delle vittime. Sono atteggiamenti che vanno codificati, magari vanno codificati in modo più elaborato e più attento e in questa norma effettivamente si dà una definizione più precisa di ciò che si deve intendere per bullismo e per cyberbullismo.

Il complesso normativo che si intende approvare responsabilizza ogni istituto scolastico, obbligandolo ad adottare un codice interno per la prevenzione e il contrasto di tali fenomeni; in uno degli emendamenti approvati al Senato si interviene proprio su questo aspetto.

Gli articoli della legge *de qua* contengono disposizioni finalizzate a coordinare i vari enti coinvolti e le famiglie, per poter ottimizzare tutti gli strumenti rieducativi e preventivi previsti dalla normativa anche con riferimento ai minori di 14 anni che, come sappiamo, non sono imputabili ma possono essere - come

giustamente detto dal relatore - destinatari di provvedimenti di carattere amministrativo. Luogo chiave di tali interventi sarà ricoperto dai servizi sociali minorili e dal tribunale per i minorenni, che dovranno comunque rapportarsi con il minore, con i genitori e con gli esercenti la potestà genitoriale. Il testo che ci accingiamo a votare è il frutto - è stato ricordato in quest'Aula - di un lavoro congiunto e sinergico tra tutte le forze parlamentari. Tale circostanza è dettata sicuramente dall'allarme sociale che i fenomeni che si intendono contrastare stanno producendo: non solo i fatti di cronaca più gravi sono il campanello di allarme di un fenomeno generalizzato - è stato ricordato quello di Willy Duarte, io conosco personalmente la famiglia di Willy che è della mia provincia; difendo alcune delle vittime di quell'episodio, in particolar modo gli amici di Willy che erano lì presenti in quel momento - ma anche gli stessi dati dell'Istat, che ha condotto in tal senso ricerche, dicono che più del 50 per cento dei ragazzi intervistati tra gli 11 e 17 anni hanno riferito di essere rimasti vittima, nel corso della propria vita, di qualche episodio offensivo, violento o irrispettoso e, ancora più grave, il 20 per cento dei ragazzi ha dichiarato di esserne stato vittima o di aver assistito a tali fenomeni con una cadenza almeno mensile. Quindi, questo per evidenziare la gravità, la ripetitività, la diffusione di questi fenomeni.

Volendo però andare nello specifico delle modifiche apportate al Senato, per non dilungarmi su quella che è stata già una discussione fatta in tale Aula, voglio interviene sulle variazioni che andremo a discutere e a votare, da qui a poco. Le modificazioni sono state apportate soprattutto all'articolo 1, comma 1, lettera *b)*, per il necessario aggiornamento delle disposizioni relative alla copertura finanziaria, perché facevano riferimento all'anno finanziario 2023, quindi è stato necessario doverle aggiornare, ovviamente, all'anno in corso; poi il comma 1, sempre del medesimo articolo 1, lettera *d)*, dove è stata disposta la soppressione del riferimento al servizio di coordinamento pedagogico, nell'ambito delle iniziative adottabili dalle regioni in attuazione della legge n. 71 del 2017, ciò è stato fatto per non vincolare l'azione in tal senso positiva delle regioni rispetto a un coordinamento che poteva sembrare ridondante; l'articolo 1, comma 1, lettera *e)*, al fine di specificare che il dirigente scolastico è tenuto ad applicare le procedure previste dalle linee di orientamento ministeriali qualora, nell'esercizio delle sue funzioni, venga a conoscenza di atti di bullismo o di cyberbullismo, precisando che i riferimenti delle condotte di bullismo e cyberbullismo, che devono essere inserite nei regolamenti scolastici, devono essere formulati sulla base di quanto previsto dalle linee di comportamento adottate dal Ministero dell'Istruzione dell'università e della ricerca, sentito il Ministero della Giustizia. Qui, correttamente, se da una parte si impone l'obbligo agli istituti scolastici di dotarsi di un regolamento finalizzato a rilevare e a contrastare gli atti di bullismo, è pur vero che a volte - lo dicevo all'inizio del mio intervento - non è semplicissimo distinguere ciò che lo è e ciò che non lo è. In questo caso gli istituti scolastici possono prendere le linee guida e concordare con i ministeri *ad hoc* quelle che devono individuare. Questa cosa è particolarmente interessante perché, in particolar modo sul cyberbullismo, se tornassimo indietro nel tempo e tentassimo di spiegare, trent'anni fa, a chi non conosceva ancora il mondo dei social che togliere contemporaneamente i *like* di una classe a un ragazzo o escluderlo da una *chat* può diventare, congiuntamente ad altro, un atto di emarginazione, se lo volessimo spiegare a qualcuno nella fase *pre-social* faremmo fatica a fargli capire perché questo costituisce violenza. In futuro, probabilmente questo avverrà con altre situazioni, cioè oggi ci sono previsioni di atteggiamenti lesivi che non riusciamo nemmeno a configurare, perché saranno il frutto di un'evoluzione sociale, oltre che un'evoluzione di approccio ai *social,* all'intelligenza artificiale e a tutto quello che ne

verrà. Quindi, è giusto che le scuole possano fare questo regolamento, ma abbiano una guida nel Ministero, che indichi quali siano le tracce.

L'articolo 2, comma 1, lettera *a)*, al fine di integrare le novelle recate all'articolo 25 in materia di misure educative - è stato poc'anzi già richiamato - rivolte minorenni, aggiunge anche il riferimento agli altri esercenti la potestà genitoriale a quello relativo ai genitori. Quindi, è un'integrazione dovuta perché, oltre ai genitori, dice che il deposito della relazione sociale va tempestivamente comunicato agli esercenti la potestà genitoriale, ma anche al curatore, al PM e ai difensori, quindi agli altri soggetti. Questo, quindi, nella fase fondamentale, che è quella della relazione sociale, va comunicato; anche se poi vedremo che, successivamente, nella fase in cui il tribunale dovrà decidere se prolungare il servizio stabilito nella casa di comunità oppure interrompere o adottare altri provvedimenti, può farlo anche senza sentire i soggetti che già sono stati avvisati, questo per evitare che ci sia un'eccessiva burocratizzazione del meccanismo. Tant'è che, poi, sempre lo stesso articolo modificato dice che è stato soppresso l'obbligo del tribunale di sentire il minore, il genitore o l'esercente la potestà genitoriale prima dell'adozione del decreto con cui si dispone, in via alternativa, la conclusione del procedimento, la continuazione del progetto educativo, l'affidamento ai servizi sociali o il collocamento in comunità. Perché questo? Perché è ovvio che nel procedimento, in particolare nella fase iniziale di indagine, i servizi sociali e tutti questi soggetti sono stati resi edotti, ma può accadere che, magari, ci sia difficoltà nello stesso tribunale nel reperire la disponibilità immediata a notificare gli atti ai soggetti interessati e quindi può adottare ugualmente queste decisioni, a tutela ovviamente del minore e di tutti i soggetti che abbiamo poc'anzi menzionato.

L'articolo 3, comma 1, inserisce la locuzione "nel rispetto dei seguenti principi e criteri direttivi", cui deve attenersi il Governo nell'esercizio della delega per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo, indicando che il Governo, nell'emanare il provvedimento governativo, dovrà tener conto necessariamente delle linee guida che sono state ben elencate e rappresentate in questo provvedimento; questa è sostanzialmente la modifica apportata.

Come già preannunciato in sede di dichiarazione di voto dal nostro presidente di Commissione, Ciro Maschio, anche Fratelli d'Italia, come diceva il relatore, insieme anche ad altri partiti, pur di arrivare a una sintesi con tutte le altre sensibilità presenti in quest'Aula, ha rinunciato a una parte delle proprie proposte, che prevedevano inizialmente misure più incisive ed efficaci sotto il profilo sanzionatorio; però ritenendo che questi provvedimenti penalmente rilevanti, invece, possano, con una forte carica deterrente, essere introdotti assieme ad altre misure in modo particolare per contrastare fenomeni criminali più gravi, quali quelli associati alle *baby gang* e alle associazioni a delinquere di stampo mafioso, al decreto Caivano e tutto quello che verrà. In questo provvedimento, quindi, si è inteso privilegiare l'aspetto preventivo ed educativo, sottolineando la gravità di alcuni comportamenti che troppo spesso sono sottovalutati o ignorati, dietro lo scudo dell'anonimato nel caso di Internet o dell'irrilevanza penale nel caso del bullismo minorile, che causano però sofferenze e afflizioni alle vittime e cicatrici che sono difficilmente rimarginabili. Siamo sicuri - ho già detto - che, con l'avanzare degli strumenti tecnologici e la modalità di approccio gli stessi, in futuro dovremo adeguare ulteriormente tali normative, ma siamo felici di aver costruito il quadro legislativo, all'interno del quale potremmo farlo *(Applausi)*.

PRESIDENTE. È iscritto a parlare il deputato Casu. Ne ha facoltà.

ANDREA CASU (PD-IDP). Grazie, Presidente, relatore, rappresentante del Governo, onorevoli colleghi. Oggi torniamo

ad affrontare un nuovo passaggio di un lungo percorso. È stato ricordato dal relatore e dall'intervento di chi mi ha preceduto; fatemi ricordare anche la senatrice Elena Ferrara, della XVII legislatura, del Partito Democratico, prima firmataria del primo provvedimento, che oggi andiamo ad attualizzare.

Io penso che sia molto importante questo aspetto. Quando avevo già avuto modo di intervenire per il gruppo del Partito Democratico nel precedente passaggio, avevo concluso il mio intervento richiamando l'aspetto forse più importante di questa legge, ossia come prevenzione e contrasto possano e debbano camminare insieme per riuscire a vivere quel senso proprio del termine "educare", che viene dall'origine antica di questa parola, nel senso di tirare fuori, di estrarre, di guidare, di strappare via delle radici questo fenomeno.

Questo è il senso della legge del 2017, dell'intervento normativo che abbiamo già discusso, del testo ulteriormente modificato che arriva dal Senato e che speriamo possa - nel più breve tempo possibile - diventare legge. Però, dobbiamo anche renderci conto delle cifre drammatiche che sono state ricordate, degli episodi continui che noi viviamo, vediamo, di cui ci accorgiamo. Ricordiamo sempre che ciò che viene denunciato, ciò che arriva alla nostra attenzione e ciò che sappiamo è sempre semplicemente la punta dell'*iceberg* di un fenomeno sommerso, infinitamente più vasto, che non viene denunciato e che non viene raccontato anche per quella vergogna e per quello stigma sociale che accompagnano questi fenomeni e che portano la persona che li subisce a trovarsi sola e a voler stare da sola di fronte alle difficoltà che si trova ad affrontare.

Da questo punto di vista è un fenomeno che sta crescendo, nonostante noi stiamo mettendo in campo un sistema sempre più attento di strumenti complessi per affrontarlo.

Allora, qui è imposta una riflessione. Noi oggi dobbiamo portare avanti questo percorso legislativo, ma forse dobbiamo alzare lo sguardo oltre i precetti di questa norma, i tanti aspetti positivi per la prevenzione del fenomeno, su quelle competenze in campo psicologico, pedagogico, di comunicazione sociale e telematiche, che possono insieme lavorare a un tavolo tecnico, che ci consenta di capire quale sia lo stato delle politiche che vengono messe in campo, il monitoraggio e, nel monitoraggio, il ruolo attivo dei destinatari del monitoraggio, cioè degli studenti, degli insegnanti e delle famiglie. Il tema del sostegno psicologico, nonché tutte quelle misure che sono contenute, sono sicuramente fondamentali, però, evidentemente, noi dobbiamo considerare che è necessario un rafforzamento complessivo dei servizi al livello territoriale, che ormai si consuma e si vive in una dimensione sia fisica che digitale.

Questo penso sia un elemento importante di questa norma, che tiene insieme bullismo e cyberbullismo, perché noi non viviamo una vita a compartimenti stagni. Non c'è una dimensione nel mondo digitale e una dimensione nel mondo non digitale, è la stessa vita, sono le stesse relazioni ed è la stessa crescita.

Certo, per noi, che ci siamo arrivati e siamo cresciuti in una dimensione analogica, è più complicato comprenderlo, ma non per i ragazzi di oggi. Basta guardare la velocità con cui un figlio o un nipote con un *device* riesce, a pochissimi anni di vita, a passare da un contenuto all'altro, la voracità con cui richiede di poter avere un *device*, perché si sente quasi privo di una parte di sé e della propria personalità nel momento in cui è disconnesso. Ecco, da questo punto di vista, per le nuove generazioni, questa distinzione non esiste.

Quindi, immaginare norme che tengano conto di questi due aspetti è già un passaggio molto importante. Tuttavia, noi dobbiamo rafforzare complessivamente tutto il presidio di servizi territoriali nei confronti delle persone, perché quegli strumenti con cui deve interagire questa legge - ed è anche questa, lo ricordo, una legge con una clausola di invarianza finanziaria (articolo 6) - siano in grado di produrre

effetti e non restare semplicemente sulla carta, come un bellissimo elenco di precetti, affinché quelle scuole, quei servizi sanitari, quei servizi territoriali, con cui dovranno interagire questi tavoli di lavoro, avranno una dotazione di risorse e di personale in grado di realizzare concretamente una gestione di servizi, che devono essere universali e rivolti a tutti, non solamente a quel bambino che ha la fortuna di essere nato in quella città o in quel quartiere di quella città dove c'è un progetto sperimentale di eccellenza.

Noi dobbiamo passare da una situazione in cui è facoltativo, volontario, possibile mettere in campo degli strumenti a una condizione in cui sia garantito, in tutte le realtà territoriali, il diritto a non essere lasciati soli in questa grande battaglia che stiamo vivendo.

Da questo punto di vista, è chiaro che è indispensabile, nei confronti di quelli che sono tutti i presidi per la salute mentale, un'attenzione più marcata a tutte le età, in tutti i passaggi, anche perché - diceva bene il relatore, mettendo in evidenza come poi, purtroppo, bullismo e cyberbullismo possono essere la porta d'accesso a disturbi ben peggiori e dalle conseguenze devastanti e in devastante crescita - è indispensabile che quei presidi, che servono ad opporsi, siano più forti.

In tal senso, io penso che sia indispensabile un passaggio, perché fino a quando si è cominciata questa discussione politica erano numeri che davano l'idea di una malattia crescente, ormai sono numeri da pandemia.

Quando ci viene detto che un ragazzo su quattro, fino a 17 anni - secondo i dati di *Save the children* -, ha vissuto almeno un episodio di bullismo nella propria vita, che ci sono tantissime ragazze e ragazzi, in età sempre più giovane, che vivono questo tipo di episodi, vuol dire che ormai siamo oltre il campanello d'allarme, ormai il suono è talmente forte da essere inarrestabile.

Quindi, ben vengano tutti gli strumenti normativi che servono a rafforzare la consapevolezza del fenomeno complessivo, anche perché c'è un tema - che in parte deve essere indagato e in parte lo stiamo affrontando - delle conseguenze di quella sensazione - lo abbiamo detto prima nel dibattito sulla cybersicurezza - d'impunità digitale, cioè dell'idea che quello che avviene in una dimensione che non è fisica, in qualche modo, sia un qualcosa di cui nessuno verrà a sapere o in cui comunque non ci sarà imputato o che comunque non genererà conseguenze.

Invece è totalmente il contrario, perché è qualcosa che, ancor di più che nella realtà non digitale, tutti possono sapere se hanno gli strumenti adeguati per arrivare a quell'informazione, perché genera conseguenze, spesso delle conseguenze ancora più gravi di quello che può avvenire in altri contesti e pertanto deve essere giustamente e correttamente sanzionato. Quando, però, le proporzioni di questo fenomeno - e qui veramente vado a concludere - hanno questi numeri, se noi li guardiamo da un lato, vediamo i destinatari di questi atti, che sono delle vittime che non devono essere lasciate sole, loro e le loro famiglie devono essere sostenuti. Tuttavia, non possiamo dimenticarci che, dietro un quarto di persone che subiscono, vi è almeno un quarto di persone che generano questi comportamenti e la nostra attenzione deve essere anche diretta ad evitare, con ogni mezzo possibile, che chi da bambino, piccolissimo, mette in campo uno di questi comportamenti così gravi, poi continui a ripeterli, senza rendersi conto della gravità di questo gesto.

La responsabilità collettiva che dobbiamo avere consiste, quindi, in non lasciare solo chi subisce, sostenerlo, aiutarlo, difenderlo, proteggerlo, trovare il modo corretto di sanzionare chi commette, ma anche scommettere sul fatto che, chi commette un atto di bullismo, un domani possa capire che sta sbagliando e cambiare i propri comportamenti; perché se noi questa partita non la giochiamo a viso aperto, rischiamo poi di soccombere, perché se questi numeri del cyberbullismo e del bullismo arriveranno ad essere, sulle gambe di una nuova generazione, i numeri delle violenze nelle nostre città, nei nostri luoghi di lavoro

o nei nostri spazi di vita adulta, noi saremo arrivati ad una situazione insostenibile.

Dato che la partita si gioca adesso, ritengo indispensabile, personalmente e politicamente, che, nel momento in cui ci occupiamo, giustamente, di una legge che specificatamente introduce precetti e strumenti, ci soffermiamo anche sull'importanza di inserire questa azione in uno scenario più ampio e di mettere in campo tutte quelle politiche che vanno nella direzione della scuola, della sanità territoriale, della salute mentale, per rafforzare tutti quei presidi che poi dovranno interagire con queste norme per evitare che restino solo sulla carta *(Applausi)*.

PRESIDENTE. Non vi sono altri iscritti a parlare e pertanto dichiaro chiusa la discussione sulle linee generali.

(Repliche - A.C. 536-B)

PRESIDENTE. Prendo atto che il relatore per la II Commissione (Giustizia), onorevole Devis Dori, e la rappresentante del Governo rinunciano a replicare.

Il seguito del dibattito è rinviato ad altra seduta.

Ordine del giorno della prossima seduta.

PRESIDENTE. Comunico l'ordine del giorno della prossima seduta.

Martedì 14 maggio 2024 - Ore 11

1. Svolgimento di una interpellanza e interrogazioni .

(ore 14,30)

2. Seguito della discussione della proposta di legge:

   CONTE ed altri: Delega al Governo per la riforma della disciplina in materia di conflitto di interessi per i titolari di cariche di governo statali, regionali e delle province autonome di Trento e di Bolzano e per i presidenti e i componenti delle autorità indipendenti di garanzia, vigilanza e regolazione. (C. 304-A)

   — Relatore: PAOLO EMILIO RUSSO.

3. Seguito della discussione del disegno di legge:

   Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici. (C. 1717-A)

   — Relatori: NAZARIO PAGANO, per la I Commissione; MASCHIO, per la II Commissione.

4. Seguito della discussione delle mozioni Casu ed altri n. 1-00280 e Iaria ed altri n. 1-00281 concernenti iniziative in materia di trasporto pubblico locale .

5. Seguito della discussione della proposta di legge:

   DORI e D'ORSO; PITTALIS ed altri; MASCHIO ed altri: Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e del cyberbullismo (*Approvata, in un testo unificato, dalla Camera e modificata dal Senato*). (C. 536-891-910-B)

   — Relatori: DONDI e DORI, per la II Commissione; CIANI e MATONE, per la XII Commissione.

La seduta termina alle 19.

IL CONSIGLIERE CAPO
DEL SERVIZIO RESOCONTI
ESTENSORE DEL PROCESSO VERBALE

Dott. Renzo Dickmann

Licenziato per la stampa alle 21,05.

Stabilimenti Tipografici
Carlo Colombo S. p. A.

19STA0090480