COMMISSIONI RIUNITE
AFFARI COSTITUZIONALI, DELLA PRESIDENZA DEL CONSIGLIO E INTERNI (I)
TRASPORTI, POSTE E TELECOMUNICAZIONI (IX)

RESOCONTO STENOGRAFICO

AUDIZIONE

4.

SEDUTA DI MERCOLEDÌ 30 GIUGNO 2021

PRESIDENZA DELLA PRESIDENTE DELLA IX COMMISSIONE
RAFFAELLA PAITA

INDICE

N. B. Sigle dei gruppi parlamentari: MoVimento 5 Stelle: M5S; Lega - Salvini Premier: Lega; Partito Democratico: PD; Forza Italia - Berlusconi Presidente: FI; Fratelli d'Italia: FdI; Italia Viva: IV; Coraggio Italia: CI; Liberi e Uguali: LeU; Misto: Misto; Misto-L'Alternativa c'è: Misto-L'A.C'È; Misto-Centro Democratico: Misto-CD; Misto-Noi con l'Italia-USEI-Rinascimento ADC: Misto-NcI-USEI-R-AC; Misto-Facciamo Eco-Federazione dei Verdi: Misto-FE-FDV; Misto-Azione-+Europa-Radicali Italiani: Misto-A-+E-RI; Misto-Minoranze Linguistiche: Misto-Min.Ling.; Misto-MAIE-PSI: Misto-MAIE-PSI.

PRESIDENZA DELLA PRESIDENTE
DELLA IX COMMISSIONE
RAFFAELLA PAITA

La seduta comincia alle 15.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso la trasmissione diretta sulla *web*-tv della Camera dei deputati.

Audizione, in videoconferenza, del Sottosegretario di Stato alla Presidenza del Consiglio, Franco Gabrielli, in qualità di Autorità delegata per la sicurezza della Repubblica, nell'ambito dell'esame del disegno di legge C. 3161, di conversione del decreto-legge n. 82 del 2021, recante disposizioni urgenti in materia di *cybersicurezza*, definizione dell'architettura nazionale di *cybersicurezza* e istituzione dell'Agenzia per la *cybersicurezza* nazionale.

PRESIDENTE. L'ordine del giorno reca, ai sensi dell'articolo 143, comma 2, del Regolamento, l'audizione del Sottosegretario di Stato alla Presidenza del Consiglio, Franco Gabrielli, in qualità di Autorità delegata per la sicurezza della Repubblica, nell'ambito dell'esame del disegno di legge C. 3161, di conversione del decreto-legge n. 82 del 2021, recante disposizioni urgenti in materia di *cybersicurezza*, definizione dell'architettura nazionale di *cybersicurezza* e istituzione dell'Agenzia per la *cybersicurezza* nazionale.

Preliminarmente faccio presente che l'audizione sarà svolta consentendo la partecipazione da remoto in videoconferenza dei deputati secondo le modalità della Giunta per il Regolamento nella riunione del 4 novembre scorso.

Faccio inoltre presente, per i deputati partecipanti da remoto, la necessità che essi risultino visibili alla Presidenza soprattutto nel momento in cui essi svolgono un loro eventuale intervento, il quale deve ovviamente essere udibile. La Presidenza non potrà infatti dare la parola ai deputati non visibili o i cui interventi non siano chiaramente percepibili. A tale fine occorre dunque assicurarsi di disporre di una connessione Internet stabile evitando, ad esempio, di collegarsi da mezzi di trasporto in movimento, condizioni che di solito rendono insufficiente la stabilità e la qualità della connessione stessa.

Ricordo che l'audizione dovrà concludersi entro le ore 16, quando riprenderanno le votazioni in Assemblea. Do la parola al Sottosegretario Franco Gabrielli e lo ringrazio per la sua presenza al fine dello svolgimento della relazione.

FRANCO GABRIELLI, *Sottosegretario di Stato alla Presidenza del Consiglio*. Grazie, signora presidente. Saluto anche il presidente della I Commissione e i componenti parlamentari della I e della IX Commissione della Camera dei deputati. Sono io che ringrazio dell'opportunità che mi è offerta di poter sinteticamente illustrare le linee che hanno portato il Governo ad adottare questo decreto-legge n. 82 su un tema così sensibile per la sicurezza del Paese. Nei tempi che la presidente ha stabilito sarò a disposizione per interazioni o, se del caso, richieste di chiarimento che potranno essere sviluppate anche in una fase successiva, qualora richiesta.

Non mi attardo su questioni che sono assolutamente all'attenzione e alla cono-

scenza di queste Commissioni parlamentari, però lasciatemi sottolineare come noi stiamo parlando di un ambito estremamente complicato della vita, non solo del nostro Paese, ma dell'intero globo. Un ambito che è complesso e che dal mio punto di vista raggiungerà nel prossimo futuro ulteriori elementi di complessità.

Solo un dato: è stato stabilito che da qui al 2030 i dispositivi interconnessi saranno oltre un trilione. Già questo numero dovrebbe farci comprendere la delicatezza, la fragilità, la vulnerabilità di questo sistema. Un sistema, un ambito, un contesto esposto a minacce delle più diversificate, da quelle che attengono al mondo tipico della sicurezza, alla criminalità organizzata e al terrorismo, ma anche e soprattutto ad attività che fanno riferimento a interessi statuali, perché il dominio digitale, il dominio cibernetico, sarà sempre più uno degli elementi sui quali si misurerà la competizione fra Stati, si misurerà lo sviluppo all'interno degli Stati. Avere la possibilità di sviluppare conoscenze, tecnologie e interazioni con queste tecnologie rappresenterà una sfida che non è del prossimo futuro, ma del tempo che stiamo vivendo.

I *target* di questa complessa situazione sono principalmente le infrastrutture critiche e le infrastrutture che attengono ai settori essenziali della vita di una comunità e di uno Stato. La recente pandemia lo ha posto alla nostra attenzione. Pensate che anche qui, per dare il senso della criticità che questo mondo ci presenta, è stato addirittura coniato un termine, « infodemia », cioè la possibilità che, oltre alla virulenza del virus naturale, l'immissione di informazioni, la gestione delle informazioni, la manipolazione delle informazioni e tutto quello che attiene al dominio digitale e al dominio cibernetico rappresenta uno dei *vulnus* più importanti della vita di una comunità e della vita di uno Stato.

Qual è lo stato dell'arte nel nostro Paese ? Mi dispiace dire che lo stato dell'arte è abbastanza critico. Basterebbero due date per farci capire come noi stiamo arrivando un po' tardi sull'argomento. In Germania l'agenzia alla quale noi traguardiamo ha visto le sue origini nel 1991. Oggi dispone di circa 1.200 persone. Senza voler evocare esempi teutonici, la Francia ha un'agenzia che si chiama Anssi che è operativa dal 2009 e che recentemente ha visto portare i suoi dipendenti, le persone che vi attendono, dalle 800 iniziali a un numero superiore a mille.

Nel nostro Paese abbiamo cominciato a renderci conto della complessità e soprattutto dell'interazione, che andava al di là delle singole responsabilità dei singoli dicasteri, solo a partire dal 2012, quando è stata collocata la responsabilità dell'azione strategica in questo campo all'interno della Presidenza del Consiglio dei ministri e specificamente nella figura del consigliere militare. Scelta ovviamente dettata più dall'urgenza che non da una visione prospettica, perché chi ha un briciolo di conoscenza di che cosa sia l'Ufficio del consigliere militare può apprezzare la distanza che c'è tra avere una determinata incombenza e quella di attendervi in maniera completa ed esaustiva. Tant'è che nel 2017, sulle ali peraltro di un'urgenza che era quella della direttiva NIS (*Network Information Security*), del 2016, che sollecitava gli Stati membri a dotarsi di strutture adeguate, il Governo di allora, prima del recepimento, nel 2018, della direttiva NIS del 2016, attua una politica volta al conferimento al comparto dell'*intelligence* della trattazione di questa materia.

Ho sempre ritenuto questa scelta una scelta obbligata dai tempi, ma certamente fortemente condizionata dal fatto di essere una scelta prospettica. Tant'è vero che, seppur – e qui lo voglio sottolineare, a merito di chi in questi anni ha lavorato in questo settore – il comparto dell'*intelligence* abbia svolto una funzione, una supplenza, un'attività assolutamente meritoria, è ovvio che ha una sua natura, una sua modalità attraverso la quale il comparto è chiamato a relazionarsi con il mondo esterno. Quando si parla di resilienza cibernetica non si può non parlare di privato, non si può non parlare di accademia, non si può non parlare di tantissimi soggetti che vivono dimensioni e dinamiche che con il comparto dell'*intelligence* hanno molto poco a che fare, non perché non vi possano essere

relazioni, ma per le modalità con le quali è possibile instaurare una relazione.

Non vorrei essere equivocato. La feroce polemica sulla famosa fondazione, dal mio punto di vista non fu un errore, ma fu la scelta necessitata di un contesto necessitato. Nel momento in cui si colloca all'interno del comparto dell'*intelligence* un settore che necessariamente deve avere una relazione esterna, necessariamente si crea uno *spin-off*, che esula da quelli che sono gli ambiti propri della dimensione di un'agenzia pubblica.

Ecco perché – qui vorrei anche superare una serie di ricostruzioni come al solito strumentali – l'agenzia non si pone in contrapposizione a niente e a nessuno. È semplicemente una scelta, che io ritengo assolutamente pertinente, che il Governo ha compiuto e che il Presidente del Consiglio ha fortissimamente voluto, volta a dare al nostro Paese una struttura che fosse nella condizione di svolgere adeguatamente e principalmente una funzione sotto il profilo della resilienza cibernetica.

Oggi, signori deputati, non solo come responsabile dell'ambito della sicurezza nazionale riferita alla sicurezza della Repubblica, per come delegatami dal Presidente del Consiglio, ai sensi della legge n. 124 del 2007, non solo per la mia esperienza di Capo della Polizia, Direttore Generale della Pubblica Sicurezza e, se mi consentite, anche di Capo del Dipartimento della Protezione civile, ma come cittadino di questo Paese, io sono fortemente preoccupato. Sono fortemente preoccupato perché, come ha detto il Ministro Colao in maniera molto netta e chiara, la stragrande maggioranza della struttura cibernetica di questo Paese sotto il profilo pubblico presenta fortissime criticità.

Ecco perché credo che la scelta del Governo di ricorrere alla decretazione d'urgenza, di recepire peraltro anche la disponibilità del Comitato parlamentare per la sicurezza della Repubblica a rispettare tempistiche estremamente compresse, risponda essenzialmente a questa esigenza, cioè di dotarci quanto prima di una struttura che dovrà essere costruita. Anche qui vorrei che fosse molto chiaro. Nel momento in cui il Parlamento del Paese convertirà il decreto-legge, comincerà in maniera significativa un percorso di costruzione che ovviamente dovrà avere tempistiche fortemente compresse.

Consentitemi di fare alcune sottolineature, per evidenziare quelle che sono state le linee che hanno reso possibile la stesura di questo decreto-legge. La prima: la parte relativa al ruolo del Presidente del Consiglio dei ministri, che è il punto di riferimento, sia in termini strategici sia in termini di linee guida, attiene a pieno titolo alla sicurezza nazionale. Per questo motivo sia la catena di comando sia il riferimento al Comitato parlamentare per la sicurezza della Repubblica non sono modalità non pertinenti, ma sono modalità che rispondono all'esigenza di collocare questa materia nell'ambito della sicurezza nazionale, al tempo stesso rendendola profondamente distinta da quella che è l'attività del comparto. Altrimenti, ricadiamo esattamente nello stesso errore del passato.

Dico questo perché, se è vero, come è vero, che l'Agenzia sarà chiamata a essere l'autorità nazionale NIS, a essere lo strumento attraverso il quale il Presidente del Consiglio dei ministri attuerà le politiche per la sicurezza cibernetica del Paese, se avrà a oggetto la costruzione della sicurezza, che è precondizione per gestire adeguatamente gli incidenti di attacchi cibernetici, è anche vero che dall'ambito d'azione dell'Agenzia deve essere completamente distinta e divisa l'azione della cosiddetta *cyber investigation*, che è attribuita alle forze di Polizia. Vorrei ricordare a me stesso che viviamo in un sistema nel quale la magistratura svolge una funzione importante, anche perché qualsiasi attacco si sostanzia sempre e comunque in un reato. L'attività dell'autorità giudiziaria è un'attività che rimarrà doverosamente distinta. A questa attività provvederanno le forze di Polizia *in primis*, in base alla direttiva Minniti del 2017, quindi la Polizia di Stato, a mezzo della Polizia postale delle comunicazioni, che mi auguro a breve avrà una direzione centrale della Polizia scientifica e della sicurezza cibernetica.

Sarà distinta anche la cosiddetta *cyber defence*, nella quale le nostre Forze armate e il mondo militare svolgono una funzione importante. Infine, ma non per ultimo, vi è il ruolo fondamentale che le agenzie di *intelligence* dovranno svolgere. È indubbio – anche qui fuori da ogni considerazione che possa apparire non politicamente corretta – che il periodo di coabitazione di questa materia all'interno del comparto ha provocato fibrillazioni nel comparto stesso, perché anche qui è innegabile che il ruolo, che era stato attribuito al NIS, di coordinamento dell'attività cibernetica, era vissuto dalle agenzie come una sorta di limitazione dell'attività delle agenzie stesse.

Allora io auspico che, chiarito l'ambito di azione dell'Agenzia, chiarito l'elemento che ha a oggetto principalmente l'attività dell'Agenzia (quindi la resilienza cibernetica), le agenzie impostino correttamente la loro attività nell'ambito di una *cyber intelligence* che, dal mio punto di vista, dovrà sempre più avere connotati non solo difensivi ma anche di attacco, perché in questo mondo, in questo ambito, l'attacco molto spesso è una modalità con la quale si gestisce meglio anche un'ipotetica difesa.

Proprio perché questa distinzione vuole essere la più chiara possibile, soprattutto per evitare che vi siano fraintendimenti, preannuncio che stiamo elaborando, anche previa sottoposizione al Comitato parlamentare per la sicurezza della Repubblica, alcuni emendamenti che hanno a oggetto proprio la definizione, che non riguarda solo la sicurezza cibernetica, ma anche questa doverosa coabitazione all'interno della sicurezza nazionale di un'agenzia che, però, ha a oggetto principalmente la resilienza cibernetica.

Come dicevo in premessa, stante la nostra condizione di grande criticità e di grande sofferenza da un punto di vista delle infrastrutture e anche, se mi consentite, della cultura cibernetica in questo Paese, è ovvio che quello sarà il principale, privilegiato e fondamentale campo di azione di questa nuova agenzia. Agenzia che però, come ho detto, avrà inevitabili *overlaps* con il mondo dell'*intelligence*, con il mondo del comparto. E non è un caso che il decreto-legge costruisca la sua architettura ordinamentale rifacendosi molto alla legge n. 124, perché prevede il ruolo fondamentale del Presidente del Consiglio, a cui vengono attribuiti – anche laddove dovesse essere nominata un'autorità delegata – alcune funzioni che sono esclusive, nonché una eventuale autorità delegata, che rappresenta nell'ordito del sistema anche il punto di confluenza e soprattutto di snodo di alcune inevitabili criticità.

Vi faccio un esempio molto semplice: l'eventualità di un incidente cibernetico. È ovvio che noi quotidianamente siamo oggetto di attacchi. Ovviamente la differenza la fa la compromissione. A seconda del tipo di attacco, di compromissione, l'attacco acquisisce un livello o una rilevanza che deve vedere *in primis* l'autorità politica, *in primis* il Presidente del Consiglio, nella condizione di poter intervenire. Allora lì ci sarà necessariamente uno snodo, perché la parte della « patologia fisiologica » sarà rimessa in mano all'Agenzia attraverso il CSIRT (*Computer Security Incident Response Team*) italiano, attraverso il Nucleo di sicurezza cibernetica (NSC) – che, come avete visto, è stato previsto da una legge primaria – che gestirà quella che io chiamo la « patologia fisiologica », cioè l'attività che non comporterà situazioni particolarmente complicate.

Nel momento in cui quell'attacco comincerà ad avere una connotazione fortemente lesiva della sicurezza nazionale, è ovvio che il livello sale. Anche da un punto di vista della composizione della struttura che accompagnerà il Presidente del Consiglio nella decisione, si può vedere come – in base a quanto prevede il decreto-legge – si passerà dal CIC (Comitato interministeriale per la *cybersicurezza*) al CISR (Comitato interministeriale per la sicurezza della Repubblica), che ovviamente incardinerà tutta la sua attività nell'ambito della salvaguardia delle informazioni che sono tipiche di questo mondo particolare.

Dico questo perché, a volte, anche sentendo i commenti a valle della pubblicazione del decreto-legge, molti – se non molti, alcuni – hanno sottolineato questa sorta di parallelo tra il mondo del com-

parto e il mondo dell'agenzia, quasi a voler dire: « Ma allora perché si è fatta questa distinzione ? » Si è fatta questa distinzione volutamente perché noi immaginiamo che questa agenzia debba gestire tutta una serie di compiti che con il comparto hanno poco o nulla a che fare, ma al tempo stesso non bisogna cadere nell'errore di immaginare che questa agenzia e le materie che tratterà non avranno inevitabili ripercussioni anche sulla sicurezza nazionale. Ecco perché, secondo me, era fondamentale stabilire, anche dal punto di vista dell'architettura della responsabilità politica, uno snodo che noi abbiamo individuato *in primis* nel Presidente del Consiglio dei ministri, ma anche nell'Autorità delegata, laddove costituita.

Mi permetto di svolgere alcune sottolineature e poi mi taccio, rimettendomi non solo al vostro giudizio ma anche alla vostra interlocuzione. Uno degli aspetti che io sottolineo positivamente di questo decreto-legge è che, per la prima volta dal 2018, è stata individuata un'unica Autorità nazionale, in base alla direttiva NIS. In questo momento abbiamo 23 autorità nazionali NIS. Capite bene come, anche nel rapporto con le autorità unionali, avere un Paese che ha 23 Autorità NIS non solo è poco credibile ma anche poco funzionale, anche perché – vi fornisco anche questa informazione – moltissime di queste Autorità NIS non hanno ancora comunicato il referente. È anche complicato stabilire se, nell'ambito dell'azione di queste autorità, si stanno seguendo quelle che sono le direttive che l'Europa ci ha indicato.

Questa agenzia sarà l'Autorità nazionale NIS, ma lì è stata compiuta, secondo me, un'operazione che non può non tenere conto di quello che è stato fatto e soprattutto anche della complessità del nostro sistema. Sono state create le Autorità di settore, in modo tale che il MISE (Ministero dello sviluppo economico), il MIT (Ministero delle infrastrutture e dei trasporti) e le regioni continuino ad avere un ruolo importante nell'ambito del loro campo di competenza, raccordandosi con l'Autorità nazionale NIS.

Questo lo si farà – la norma nel decreto-legge lo prevede – attraverso una sorta di Comitato operativo, di un Comitato di raccordo, che consentirà di tenere conto delle sensibilità che appartengono agli ambiti propri. Pensate, ad esempio, al tema regionale dell'acqua pubblica o della sanità, che impattano necessariamente su questioni per le quali esistono sensibilità che non possono non essere tenute in debita considerazione; ma al tempo stesso queste sensibilità, anche e soprattutto nelle relazioni con le autorità unionali, non possono trovare che un punto di sintesi, costituito dall'agenzia.

Vi sono due grandi novità – io le considero tali – che potrebbero rappresentare anche una sorta di *benchmark* o comunque un modello a cui guardare. Un aspetto che fin dall'inizio ho cercato di sottolineare a tutti, e debbo dire che il Presidente del Consiglio è stato il primo grande recettore, è che ci sono alcuni settori della vita del Paese che richiedono professionalità di grandissimo livello, le quali devono essere anche retribuite adeguatamente al grandissimo livello che esprimono. Peraltro, in un settore nel quale la competizione nel mercato del lavoro esterno – ciò è assolutamente a conoscenza dei signori parlamentari – presenta – soprattutto nel nostro Paese – con riferimento alla componente tecnica, molto spesso, una grande vulnerabilità. In questo senso sono strettamente collegate le modalità di acquisizione di queste professionalità.

Io rassegno a voi una considerazione un po' amara: questo Parlamento, nel 2019, con la conversione del decreto-legge n. 105, ha istituito il perimetro di sicurezza cibernetica. È un modello che, peraltro, con grande fatica, si è riusciti a portare a termine proprio nelle settimane scorse e che prevede un architrave fondamentale, che è il Centro di valutazione e certificazione nazionale (CVCN). Ad oggi non solo non è operativo, ma i famosi 70 ingegneri che avrebbero dovuto essere assunti, non sono state ancora assunti. Ora io non dico che dobbiamo recriminare per il fatto che i tedeschi nel 1991 abbiano istituito l'agenzia che noi oggi costruiamo o che l'abbiano istituita i francesi nel 2009, dico semplicemente che non possiamo più permetterci di

perdere tempo su una tematica che credo debba invece viaggiare, se non alla velocità della luce, almeno con tempistiche diverse da quelle a cui siamo abituati.

In questo senso l'altra grande novità è che l'agenzia sarà composta non soltanto da persone assunte a tempo indeterminato, ma anche, per un'aliquota significativa, da persone assunte a tempo determinato, a contratto, con contratti privati, perché questo è un mondo nel quale le professionalità e le conoscenze hanno un *turnover* pazzesco. Se noi non stiamo al passo, la sfida che abbiamo davanti è una sfida che andrà perduta. Ma – potrebbe essere l'obiezione – queste persone sono da « rottamare » ? No, l'ambizione dell'Agenzia è anche quella di creare un *workforce* di un certo tipo, che può trovare un'adeguata ricaduta in una pubblica amministrazione estremamente anemizzata da questo punto di vista. Quindi il decreto-legge risponde a questa esigenza di fare presto, di dotare il Paese di questo sistema che attenga alla resilienza.

Io non vorrei banalizzare, ma in questi giorni spesso ho utilizzato un esempio per far comprendere di che cosa stiamo parlando e anche per far comprendere il rapporto che esiste tra le componenti che sono chiamate a garantire la sicurezza rispetto all'agenzia, la quale sarà chiamata principalmente a garantire la resilienza. L'esempio è molto banale, è quello dei furti in appartamento. Peraltro è un problema estremamente grave, delle cui attività di contrasto ho avuto la responsabilità per cinque anni, come Capo della Polizia. Che cosa succede nei furti in appartamento ? Succede che il cittadino ha una legittima, doverosa, sacrosanta aspettativa che le forze dell'ordine impediscano al ladro di entrare o che, qualora malauguratamente il ladro entri in casa, sia poi assicurato alla giustizia. Ma la vera differenza – lo sappiamo tutti – la fanno un buon sistema di allarme e delle buone porte blindate. Se noi trasferiamo tutto questo nel mondo del *cyber*, noi potremmo avere degli efficienti apparati investigativi, degli efficienti apparati di *intelligence* o di difesa che contrasteranno l'azione degli *hacker* o di chi, anche e soprattutto a livello di interessi statuali, porterà attacchi, ma se noi non ci dotiamo di un sistema performante, di un sistema che abbia la capacità di resistere almeno a un certo tipo di attacchi, noi la battaglia l'abbiamo già perduta. In questo senso è ovvio che un ruolo fondamentale ce l'avrà questa grande interconnessione con tutti gli attori.

Mi taccio veramente per rivolgervi una preghiera. È ovvio che ci saranno gli emendamenti. Gli emendamenti sono una ricchezza anche del dibattito parlamentare, anche perché se così non fosse, si farebbero le cose « a scatola chiusa ». Vorrei sottolineare due esigenze. La prima. Questa agenzia ha nulla o poco a che fare con la legge n. 124. Aprire un dibattito sulla legge n. 124 innestandolo nell'ambito di questo tipo di considerazioni rischierebbe di portarci lontano, anche se io appartengo alla categoria di chi – avendo lavorato nel 2007 alla stesura della legge n. 124 – ritiene che sia arrivato anche il tempo per rivisitare tale legge. Ma, come direbbe Lucarelli, questa è un'altra storia !

Un'altra considerazione: in questo ambito non si dovrebbe andare a ricercare la sottolineatura delle competenze dei vari dicasteri con i vari « fatto salvo ». Qui si fa salvo tutto e poi si rischia di compromettere tutto. Oggi è il tempo della costruzione di qualcosa di nuovo e di diverso, in cui il « fatto salvo » passa anche da una intelligente cessione di ipotetica sovranità, perché troppo spesso la ricerca e la sottolineatura di ambiti di competenza hanno creato problemi nel rendere possibile percorsi che, soprattutto come nel mondo del dominio cibernetico, hanno bisogno di visione, hanno bisogno di affrancamento da logiche di cortile, da logiche che tendono a salvaguardare l'esistente, non avendo il coraggio di aprirsi, invece, a nuove frontiere e a nuove sfide.

Mi scuso per il tempo che vi ho sottratto.

PRESIDENTE. Grazie, Sottosegretario Gabrielli. Do la parola ai deputati che intendano porre quesiti o formulare osservazioni.

VINCENZA BRUNO BOSSIO. Grazie, Sottosegretario. Ha fatto bene a inquadrare lo stato dell'arte della *cybersecurity* in Italia e di come siamo arrivati tutto sommato tardi, nel 2012, anche se devo dire che abbiamo provato a recuperare questo ritardo. La legge sul perimetro della sicurezza nazionale e adesso l'istituzione dell'Agenzia sono sicuramente delle scelte che ci hanno fatto recuperare tempo, almeno dal punto di vista normativo e organizzativo.

Io condivido molto quello che lei ha detto a proposito della separazione tra i diversi livelli, di come l'Agenzia sia sostanzialmente predisposta alla resilienza rispetto agli attacchi, distinguendo tra il momento proprio del crimine cibernetico e quello dell'*intelligence* cibernetica. Questo va benissimo.

Quello su cui ho dei dubbi è come si tiene insieme tutta la parte organizzativa attuale del sistema della resilienza cibernetica. Non voglio parlare né di crimine né di *intelligence*, ma di resilienza, perché il perimetro della sicurezza nazionale aveva istituito alcuni comitati che comunque adesso sono stati in parte superati, assorbiti, riarticolati con l'Agenzia. E questo è un primo tema.

Si parla delle Autorità di settore, ma poi per esempio si lascia il « fatto salvo » per quel che riguarda il Ministero dello sviluppo economico. La resilienza cibernetica non può riguardare solo la pubblica amministrazione; naturalmente deve riguardare molto anche le imprese. Io le chiederei personalmente, se non fosse un tema che riguarda tutti i cittadini, di avere un quadro preciso di tutta questa riorganizzazione. Nonostante io mi stia occupando dal 2013, da quando sono stata eletta – con le mie scarse competenze, come parlamentare – di questo tema e soprattutto del tema che dovrebbe riguardare l'Agenzia, cioè la resilienza, devo riconoscere che questi passaggi che abbiamo fatto, che sicuramente sono stati importanti e significativi, devono ancora essere chiariti bene. Io ricordo tutta la discussione faticosissima che abbiamo svolto, però va evidenziato che ci sono stati dei ritardi pazzeschi nell'attuazione.

Adesso c'è l'Agenzia. Si dovrebbe riorganizzare e velocizzare. Però capire meglio come questa riorganizzazione possa funzionare e anche con quale cronoprogramma, secondo me è fondamentale, perché altrimenti anche noi rischiamo – parlo come parlamentare – di non poter dare il nostro contributo rispetto a quello che, sono d'accordo, è il tema più strategico. Vedo che l'Agenzia è anche all'interno del Comitato per la transizione digitale. È fondamentale, però credo che tutte queste cose vadano inquadrate meglio, perché non si capisce cosa viene superato e cosa rimane e soprattutto quali saranno effettivamente le diverse responsabilità.

PRESIDENTE. Grazie, onorevole Bruno Bossio. Nel darvi la parola vi ricordo che c'è l'Aula alle ore 16, quindi vi chiederei massima sintesi per dare poi la possibilità al Sottosegretario Gabrielli di rispondere compiutamente.

GENNARO MIGLIORE. Vorrei porre delle domande molto schematiche, anche perché ritengo sia assolutamente apprezzabile il punto di avanzamento raggiunto dal testo del decreto-legge. Partirei da alcune considerazioni che ha svolto il Ministro Colao sostenendo – non so se questo corrisponde nella quantità – che il 95 per cento della pubblica amministrazione è privo di sicurezza cibernetica. Evidentemente, è un dato gigantesco, rispetto al quale credo che la tempistica che lei evocava è fondamentale.

Ora, poiché lei ha parlato del Centro di certificazione che da due anni non si realizza, volevo chiederle in maniera secca: è prevista anche la realizzazione di un *cloud* nazionale, di un antivirus nazionale, di un *blockchain* nazionale sovrano, in modo tale da garantire che vi possa essere, almeno per la parte pubblica, un accesso diretto e univoco a questi sistemi di protezione cibernetica ?

La seconda domanda è la seguente, proprio per essere più rapidi: quale rapporto ci sarà con quelle strutture di controllo

cibernetico a livello europeo – tipo il sistema CyCLONe – che fino ad oggi hanno rappresentato soprattutto un collegamento della parte dell'informazione ? È previsto che ci sia, per esempio, con l'Agenzia francese un interscambio da questo punto di vista anche a livello europeo, visto che alcuni attacchi – quasi tutti – hanno una portata superiore ? Poi le chiedo se può chiarirmi come è finita la vicenda della *back door* di *SolarWinds Orion*, che sostanzialmente credo sia stato il più grande attacco cibernetico degli ultimi anni, rappresentando, quindi, anche un *case study* molto importante per questo tipo di attività.

PRESIDENTE. Grazie, onorevole Migliore. Onorevole Mollicone.

FEDERICO MOLLICONE. Presidente, raccoglieremo il suo invito, però considerando l'importanza del tema e il fatto che vi sono vari scenari da affrontare, un po' di attenzione va posta. Il decreto-legge in esame mette insieme, dottor Gabrielli, le competenze e le capacità disperse in vari organismi e gangli dello Stato, il DIS (Dipartimento delle informazioni per la sicurezza), l'AgID (Agenzia per l'Italia digitale), il MiSE, riformando di fatto un'architettura istituzionale che spesso non ha permesso la costruzione di uno scudo cibernetico adeguato alla sfida della digitalizzazione massiva che la pandemia ha portato.

Rileviamo di certo il ruolo di controllo attribuito al Copasir (Comitato parlamentare per la sicurezza della Repubblica), che è anche corretto nel lessico costituzionale e parlamentare, e quindi di fatto al Parlamento: dalle nomine di direttore e vicedirettore alla pianta organica, al bilancio, come avviene per le agenzie di *intelligence*. Non è chiaro, però, quale sia l'ambito di competenza di chi resterà al DIS e quali siano le modalità di comunicazione tra la nuova Agenzia e l'*intelligence*. Inoltre non appare chiaro se coloro che transitano dal DIS all'Agenzia possano poi tornare indietro, cosa che ovviamente ci appare inopportuna.

Nell'esame del provvedimento, poi, rileviamo alcuni punti fondamentali. Il Piano nazionale di ripresa e resilienza (PNRR) ha fra i propri obiettivi fondamentali la digitalizzazione: ne rappresenta un terzo. La digitalizzazione della pubblica amministrazione e delle imprese porta con sé anche rischi informatici. L'Agenzia può essere controllore del fatto che ogni euro speso sia anche moltiplicatore dei livelli di sicurezza cibernetica, tanto più che le valutazioni del Procurement ICT (*Information and communication technology*) da parte del CVCN passeranno dal MiSE all'Agenzia.

L'istituzionalizzazione del dialogo col mondo industriale è necessaria**.** Come si pone relativamente alla costituzione di un comitato scientifico interno di *partnership* pubblico-privato tra soggetti pubblici e soggetti privati e accademici ? Questo è l'altro quesito.

Riteniamo poi sia necessario prevedere in capo all'Agenzia anche compiti inerenti alla sicurezza della *supply chain* e degli appalti aggiudicati dai soggetti non inclusi nel Perimetro di sicurezza nazionale cibernetica: in poche parole, un sistema preliminare di qualificazione e certificazione atto a consentire alle stazioni appaltanti di attribuire agli operatori economici, previa verifica tecnica e regolamentare, una specifica attestazione per la partecipazione alle gare. Una *white list*, come già descritta da accademici e analisti, è richiesta da molti operatori nazionali di eccellenza (una sorta di NOS tecnico).

Potrebbe essere utile dedicare una zona economica speciale, poi, alle aziende della *cybersicurezza*, spingendo attraverso sistemi di vantaggi fiscali le realtà produttive a insediarsi in un distretto specifico, anche coinvolgendo la Difesa e le Forze armate; fare quindi in modo che l'Agenzia diventi anche una sorta di soggetto pianificatore di questo comparto.

All'articolo 7, comma 1, lettera *n)*, del decreto-legge, compare per la prima volta nell'ordinamento italiano il concetto di « risposta agli attacchi *cyber* ». Tale assunto andrebbe meglio definito: è infatti necessaria maggiore chiarezza, per evitare che vi siano difficoltà interpretative o dubbi di natura giuridica sulle regole d'ingaggio di questo tipo di operazione. In particolare,

dottor Gabrielli, bisogna chiarire se questo tipo di operazioni rappresenti o no un'esclusiva nell'ambito *cyber defence*, e quindi prerogativa delle strutture delle Forze armate; se l'Italia offra soluzioni tecniche per portare azioni di deterrenza e reazione in dote all'Alleanza atlantica, che ha recentemente chiarito che l'attacco *cyber* implica la possibilità per il membro NATO attaccato di invocare l'articolo 5 del Trattato; il ruolo dei soggetti privati. Questo è un aspetto che riteniamo molto importante perché attiene alla sicurezza nazionale.

PRESIDENTE. Grazie, onorevole Mollicone. Onorevole Prisco.

EMANUELE PRISCO. Grazie, presidente. Molto brevemente, vado direttamente alle domande. Con riferimento all'articolo 7, dove si parla delle funzioni dell'Agenzia, viene utilizzato un termine piuttosto « stretto » sugli ambiti operativi, che è quello degli incidenti. La domanda è se obiettivamente non convenga allargare un po' il campo a tutti gli eventi che hanno connessioni dirette o indirette con la *cybersicurezza*.

Per quanto attiene al Nucleo di *cybersicurezza* e a tutta la partita della condivisione delle informazioni rispetto alle minacce di attacco, vorrei capire come si sostanzia, anche nei rapporti con la normativa della *privacy*, oppure se si sta immaginando di utilizzare uno schema analogo a quello che si utilizza nella legge n. 124 del 2007, quindi una norma simile a quella sul segreto d'ufficio.

L'altra questione l'ha menzionata prima il collega Migliore: se vi è l'intenzione di costituire – essendo sostanzialmente questo un diritto dinamico, per cui riusciamo a fare una previsione oggi, ma probabilmente tra sei mesi bisognerà farne un'altra perché lo scenario di attacco e di difesa sarà completamente cambiato – un *cloud* nazionale sovrano detenuto dall'Italia, per la pubblica amministrazione ma anche per le aziende strategiche che operano in Italia e all'estero.

PRESIDENTE. Grazie, onorevole Prisco. Onorevole Tofalo.

ANGELO TOFALO. Grazie, presidente. Salve, sottosegretario. Io ho due considerazioni, una dal punto di vista tecnico e una dal punto vista politico. Dal punto di vista tecnico i colleghi mi hanno preceduto, in particolare la collega Bruno Bossio, con la quale da dieci anni seguiamo questi temi; quindi guadagno tempo. Vorrei un chiarimento: va bene la UE, però nel decreto-legge non si parla dei rapporti con la NATO: c'è un po' di ambiguità. Vorremmo capire – sono anche relatore ai fini dell'esame in sede consultiva sul provvedimento in Commissione difesa – questo punto nei rapporti con i tavoli internazionali per quanto riguarda la *cyber defence*; e poi, come anticipato dal collega Mollicone, cosa resta effettivamente al DIS da un punto di vista prettamente tecnico.

Da un punto di vista politico, e questa è la cosa più importante, lei dice che ci troviamo nell'ambito della sicurezza nazionale, ma al tempo stesso non parliamo dell'ambito *intelligence* e rischiamo di impelagarci nella legge n. 124 del 2007. Giusto, rischiamo di impelagarci; però è stata fatta molta confusione, soprattutto nell'ultimo anno e mezzo, su questa famosa Agenzia, fondazione, istituto. Io credo in un Parlamento sovrano. Ricordo a tutti che l'idea del Governo Renzi viene portata avanti nel Governo Gentiloni, e viene poi rimodificata con accordo al Copasir e rimessa nel Governo Conte.

Al netto di tutte quelle che sono le considerazioni politiche, questa profonda discussione nasce nel 2009-2010, Governo Berlusconi IV, dove devo dire che un illuminato dottor Gianni Letta, che ricopriva il ruolo che oggi lei ricopre, vedendo il futuro aveva fornito una linea concordata con il Parlamento sovrano e con l'Esecutivo. Aveva detto: « La legge n. 124 del 2007 prevede che le minacce cibernetiche non si possono sovrapporre; l'*intelligence* deve crescere in questa cosa ». Governo Monti, Gianni De Gennaro, stessa linea, persegue e rafforziamo col decreto del 2012. Governo Letta, Governo Renzi, Governo Gentiloni, decreto cosiddetto Gentiloni in accordo con il Copasir, Parlamento sovrano, rafforziamo ulteriormente l'*intelligence*, nella speranza che

la maturità politica portasse dei risultati. Ci siamo confrontati, io ero in opposizione dura con l'allora (altro illuminato) Autorità delegata Marco Minniti, convinto su questa linea.

Oggi confusione politica, arriva il Governo Draghi, un Copasir un po' « imballato » che litiga sulla presidenza e lei dichiara pubblicamente (a mio avviso, non lo so, forse fare il tecnico è una cosa e fare il politico un'altra cosa): 2016, peccato originale. Quella fu una scelta del Parlamento sovrano perché le agenzie erano in fibrillazione. Allora decide il Parlamento sovrano o facciamo decidere alle agenzie cosa vogliono fare della sicurezza nazionale ? La sicurezza cibernetica rientra pienamente – siamo tutti concordi – per legge nell'alveo della sicurezza nazionale. Secondo me questa Agenzia è un passo in avanti per tutta la pubblica amministrazione. Ci sono Ministeri come l'Interno, e lei ne è fautore e ha fatto di questo Ministero il primo in assoluto rispetto a tutti gli altri. La Difesa ha « galoppato » tanto, il MiSE ha « galoppato » tanto. Ci sono altri Ministeri che non hanno « galoppato ». Noi invece facciamo fare dei passi indietro al comparto *intelligence*. In dieci anni forse siamo stati immaturi nell'andare a creare un'agenzia che facesse ricerca informativa *intelligence* all'interno del dominio cibernetico sul modello americano, proprio per queste eterne frizioni interne. Non sto attribuendo a lei questa, a mio avviso, non giusta conclusione, la sto attribuendo all'immaturità della politica. Va bene così, ma poi in quell'ambito che facciamo ?

Io mi auguro allora, e spero che qui il Parlamento si esprima, che resti nel DIS un nocciolo per gestire bene tale materia. Altrimenti va bene, la Difesa fa un passo avanti, l'Interno fa un passo avanti, il sistema Paese fa un passo avanti, ma l'*intelligence* a mio avviso oggi compie un notevole passo indietro.

PRESIDENTE. Grazie, onorevole Tofalo. Onorevole Zanella.

FEDERICA ZANELLA. Cercherò di essere molto sintetica, anche se ovviamente ci sarebbero tante cose da dire. Molto ha detto la collega Bruno Bossio e condivido la necessità di risposte sui tempi. È ovvio ed evidente che proprio su questa dualità – speriamo « sinergia », ma per ora un po' « dualità » – tra DIS e la nuova Agenzia, quindi tra le funzioni del comparto e l'Agenzia, ci sarebbero molte domande. Lei ha declinato abbastanza bene queste funzioni, ci sarebbero parecchie domande sulla declinazione. Se vuole specificare qualcosa in più, anche rispondendo al collega, ci farebbe molto piacere.

Però, venendo proprio a una domanda specifica che si aggancia in effetti ai tempi, lei giustamente (era una criticità che noi avevamo più volte puntualizzato) ha sottolineato come il CVCN di fatto non solo non sia stato operativo, ma non abbia neanche acquisito le professionalità necessarie. Come pensate di farlo in breve tempo, visto che bisognerà attivarsi ? Pensate di riuscire ad ottenere un maggior successo proprio grazie ai contratti privati ?

Secondariamente le vorrei chiedere un'altra cosa. C'erano stati una serie di *vulnera* che erano stati sottolineati anche dalle aziende per quanto riguarda il CVCN. Visto che a questo punto acquisite tutto voi, vi interfaccerete con i privati sotto questo profilo ? Grazie.

PRESIDENTE. Grazie, onorevole Zanella. Onorevole Perego.

MATTEO PEREGO DI CREMNAGO. Grazie, presidente. Grazie, sottosegretario. Immagino che lei avrà avuto occasione di visitare il Comando per le operazioni in rete (COR) della Difesa, dove si può osservare come gli attacchi, di origine statuale e non, alle nostre infrastrutture siano un tema frequente, costante e quotidiano. La mia domanda riguarda la fase *offense*: vorrei sapere se lei ritiene che i *cyber attack* dovrebbero essere condotti da strutture della Difesa o se invece tali strutture debbano far capo anche alla Presidenza del Consiglio.

Credo che questo possa evidenziare dei rilievi rispetto all'articolo 11 della Costituzione, mai affrontato su questo tema, perché se devo pensare all'attacco di natura

ordinaria condotto dalle Forze armate ci sarebbe una catena di comando così lunga che ovviamente nel dominio *cyber* non si può applicare. Quindi delle due cose l'una: o demandiamo alla Difesa di occuparsi della parte *offense* che, come lei ha detto bene, è una forma di difesa, però anche lì dovremmo cambiare completamente la catena di comando e di autorizzazione; o invece, se si dovesse far capo alla Presidenza del Consiglio, sarebbe necessario uno strumento per il quale l'autorizzazione sia immediata. Non si può pensare di concertare sull'opportunità o meno, perché il dominio lo richiede. Di questo credo che si parli un po' troppo poco: vorrei un suo parere in merito. Grazie.

PRESIDENTE. Grazie, onorevole Perego. Onorevole Nobili per l'ultimo intervento, e poi abbiamo dieci minuti per la risposta del sottosegretario. Però io lo dico, anche per tutti i colleghi: nel caso in cui doveste ritenere necessario un ulteriore approfondimento, domani possiamo operare un'integrazione dell'ordine del giorno e trovare comunque delle disponibilità. Vediamo come riusciamo ad incastrare e poi decidiamo insieme.

LUCIANO NOBILI. Sì, molto rapidamente, perché molte delle questioni sono state evidenziate anche da altri colleghi e perché la relazione è stata molto esaustiva. Anzi, ringrazio il sottosegretario anche per la capacità di essere molto franco nell'esposizione e di offrirci sia i vantaggi che l'Agenzia rappresenterà, sia gli ambiti e le distinzioni sui temi della *cyber investigation*, della Difesa e di altre questioni che restano invece ambiti separati.

Io ho due questioni da aggiungere. La prima è la seguente: l'Agenzia è un pezzo del PNRR e il decreto-legge la realizza, ma una parte rilevantissima – lo si ricordava – è tutto il tema della digitalizzazione del Paese, che deve camminare insieme. Gli obiettivi che il Ministro Colao si è dato sono obiettivi che io definisco insieme molto ambiziosi, ma anche molto pragmatici nella loro realizzazione: l'anticipo al 2026 della scadenza del PNRR e degli obiettivi che il *Digital Compass* europeo poneva al 2030, cioè un *gigabyte* al secondo per famiglie e imprese, un obiettivo che se oggi guardiamo la situazione è molto ambizioso, ma che dovremo fare di tutto per realizzare. Sul *cloud* si richiamavano, anche se toccano incidentalmente l'attività dell'Agenzia, i temi che abbiamo sulla pubblica amministrazione (li menzionava il collega Migliore) che riguardavano *SolarWinds*; al riguardo, ricordo che anche quest'anno l'Irlanda, pochi mesi fa, ha subito un attacco *cyber* che in particolare ha riguardato il settore sanitario, molto rilevante, ed è un tema di criticità che il Ministro Colao ha richiamato più volte.

La questione è, da una parte, che ruolo può avere l'Agenzia, se l'avrà, se potrà averlo, nell'accompagnare questo percorso di digitalizzazione e il mantenimento di tempistiche molto serrate. Lì c'è anche un tema di possibile duplicazione di investimenti pubblici, c'è una mappatura molto seria da realizzare. Dall'altra parte cosa si può fare – anche sul tema del *cloud* il Ministro Colao ha indicato una strategia molto chiara, il Polo strategico nazionale entro il 2022 e così via, ricorrendo anche a tecnologie internazionali in questo momento –, e anche l'Agenzia che ruolo può avere per il potenziamento delle aziende italiane che operano nel settore della *cybersicurezza*. È sicuramente strategico aiutare il comparto delle imprese nazionali che lavorano su questo ad un avanzamento tecnologico importante, per fare in modo che poi quelle porte blindate e quegli allarmi che lei citava possano essere anche patrimonio tecnologico nazionale. Grazie.

PRESIDENTE. Grazie, onorevole Nobili. Do ora la parola al sottosegretario Gabrielli per la replica, avendo chiarito in premessa che domani mattina noi eventualmente potremmo anticipare la Commissione oppure far slittare qualche cosa, se lei è disponibile; se no concordiamo un altro momento.

FRANCO GABRIELLI, *Sottosegretario di Stato alla Presidenza del Consiglio*. Intanto io faccio riserva di mandare all'onorevole Bruno Bossio il cronoprogramma. Noi ci

siamo un po' esercitati nel cronoprogramma perché, come ho detto prima nella mia esposizione, siamo consapevoli che, al di là di quello che poi sarà l'esito della conversione in legge, il grosso, anzi il più, dovrà essere fatto a valle per rendere esecutive le cose che il Parlamento ci consegnerà.

Senza alcuna vena polemica, onorevole Tofalo, io rivendico la mia natura tecnica ma anche la mia estrema franchezza, e le pongo questa domanda retorica: se a 61 anni, raggiunta la responsabilità di mettere mano a un settore molto, molto limitato, che è quello della sicurezza della Repubblica, io avessi trovato una situazione armonica, come lei ha rappresentato, all'interno del comparto, tra il DIS e le agenzie, io mi sarei messo nella ventura di mettere mano a una cosa i cui esiti sono così complicati ? Le do la risposta: no, perché la situazione del comparto, non dell'empireo mondo, del comparto, con riferimento al tema della *cybersicurezza*, per le cose che erano state definite sotto la responsabilità dei Governi che lei ha citato e sotto il sovrano Parlamento, era assolutamente critica. Si era creato un meccanismo ipertrofico in capo al DIS che stravolgeva completamente la legge n. 124 del 2007 ed il suo spirito, e aveva prodotto e stava producendo grandissime fibrillazioni all'interno del comparto, perché le agenzie rivendicavano legittimamente un'operatività che molto spesso collideva con una modalità di gestione da parte del DIS, che non l'incapacità, ma la grande capacità delle persone che erano state chiamate a svolgere quella funzione aveva determinato.

Oggi proviamo a ripristinare una condizione nella quale – faccio riferimento anche ad alcune considerazioni che sono state fatte e che sono state ribadite da lei e da altri parlamentari – è fuori discussione che alcuni elementi, a partire dalle nostre Forze armate, dai rapporti nell'ambito della NATO, dovranno essere mantenuti nell'alveo delle rispettive competenze, perché se noi introduciamo meccanismi o modalità di approccio che confondono i ruoli e le funzioni, allora si rischia di fare della grande confusione.

Per cui io credo, per l'esperienza che ho di questo settore, che l'Agenzia non sarà un elemento di indebolimento del comparto: anzi, sarà un elemento di rafforzamento del comparto, perché il comparto tornerà a fare quello che deve fare, cioè a svolgere una funzione di *intelligence* per la sicurezza nazionale in determinati ambiti e contesti; e peraltro, avendo ottenuto da parte del Ministero dell'economia e delle finanze anche una disponibilità ad incrementare, in prospettiva, nella prossima legge di bilancio, delle dotazioni economiche che rendano la parte operativa dell'*intelligence* adeguata alla sua funzione.

Ritornando a quello che diceva l'onorevole Bruno Bossio, a cui farò avere il cronoprogramma, e lo stesso a tutti voi, vorrei che voi tutti faceste con me una sorta di considerazione: noi non siamo in presenza di una *tabula rasa*, perché se noi fossimo in presenza di una *tabula rasa* costruiremmo le architetture che vogliamo. Qui è in discussione il fatto di modellare un sistema che, in primo luogo, deve fare i conti con quello che esiste, in secondo luogo deve evitare in maniera assoluta che si realizzino delle soluzioni di continuità, perché se è vero che quello che preesiste non è la perfezione, è anche vero che molto è stato fatto. Sarebbe un suicidio e un delitto realizzare qualche cosa che vada in conflitto o che non consenta di proseguire un percorso intrapreso.

Tutto questo ovviamente ha una serie di criticità. Dal punto di vista del Nucleo per la sicurezza cibernetica le abbiamo risolte, e peraltro gli abbiamo dato per la prima volta una veste in termini di norma primaria, perché il Nucleo per la sicurezza cibernetica vedeva la sua fonte in un decreto del Presidente del Consiglio dei ministri, mentre adesso vede la sua fonte in una norma primaria; ed è dal nostro punto di vista uno snodo fondamentale, perché è quello snodo a cui facevo riferimento prima. È lo snodo a tal punto, che il Nucleo per la sicurezza cibernetica, nel momento in cui aumenta la perniciosità dell'attacco, segue l'attività dell'architettura e quindi diventa il soggetto tecnico di cui si avvale addirittura il CISR, a significare che noi non

depotenziamo il sistema ma proviamo a rafforzarlo.

Per quanto riguarda le relazioni internazionali è ovvio che l'Agenzia andrà a sostituirsi, salvo le competenze specifiche nell'ambito di consessi specifici come possono essere quelli NATO, a tutte quelle che oggi erano le relazioni in capo al DIS, per quelle che erano anche le attività nell'ambito della resilienza cibernetica.

Il tema del personale del DIS. Qui vanno distinte delle cose che saranno oggetto di alcuni emendamenti, che proporremo. Ma che sia chiara una cosa: tutto il personale che è stato assunto al DIS per svolgere funzioni che fanno riferimento alla *cybersicurezza* transiteranno nell'Agenzia, senza se e senza ma, non potrebbe essere altrimenti. Sono persone che sono state selezionate; e peraltro il mantenimento di livelli stipendiali che non possano far temere a queste persone una situazione di nocumento personale nasce, non solo perché si vuole, come dicevo prima, dare una giusta remunerazione a chi svolge funzioni di altissimo livello, ma anche per creare un meccanismo osmotico che consentirà a queste persone di transitare nell'ambito della nuova Agenzia.

Sono pienamente d'accordo sul tema della certificazione, onorevole Mollicone: questo è un obiettivo. Uno degli obiettivi dell'Agenzia è proprio quello di essere compagna di strada dell'industria del Paese, essere compagna di strada di tutte quelle aziende che devono portare il Paese a quell'autonomia tecnologica, che è anch'essa presupposto della sicurezza nazionale. In questo senso il rapporto con le industrie private, il rapporto con le imprese, sarà una modalità assolutamente da tenere in debita considerazione. Nelle prime settimane della mia attività ho ricevuto moltissimi esponenti del mondo dell'industria privata, e tutti avevano un *refrain*: abbiamo bisogno di indicazioni certe, chiare e che siano sostenute nel tempo, perché per pianificare un programma industriale non si lavora sui mesi, non si lavora sulle settimane; addirittura quelli più seri lavorano sui decenni, cioè programmano l'attività. Avere quindi un interlocutore unico che dia indirizzi unici, chiari, e che sia il frutto di una corretta interlocuzione, credo sia un'adeguata risposta.

Il tema dell'allargamento degli eventi. Anche qui vorrei dire, con riferimento all'articolo 7 del decreto-legge, che io sono convinto – lo vedrete anche nel cronoprogramma – che tra un anno e mezzo, due anni il tagliando andrà fatto. Perché noi stiamo parlando di qualche cosa che si riferisce a un contesto in continua evoluzione, e, come ho provato a dire prima, a un contesto nel quale le modalità con le quali stiamo cercando di realizzare questa nuova struttura presentano tutta una serie di criticità, e solo, come io amo dire, il campo, solo la verifica sul campo ci può dire se la strada intrapresa è quella corretta.

Sul tema dell'*offender*: anche qui patti chiari e amicizia lunga. Io sostengo da tempo che all'Agenzia non può essere attribuita nessuna funzione che deve essere attribuita ad altri ambiti: l'*intelligence*, la *cyber investigation* e la *cyber defence*. È fuori dagli orizzonti e non potrebbe essere altrimenti, anzi si rischierebbe una confusione pazzesca, il fatto di sovrapporre le competenze delle agenzie con quelle che sono invece competenze che vengono attribuite ad altri ambiti. Questo io lo credo moltissimo.

Sul discorso del CVCN e dell'interfacciarsi con le aziende ho risposto in questo senso.

Sul tema del *cloud* sta lavorando alacremente il Ministro Colao, e noi tutti auspichiamo che esso possa essere realizzato in un tempo breve.

Credo di aver risposto sul tema del personale DIS, ma ripeto: siccome questo tema l'onorevole Mollicone l'ha sollevato correttamente, perché ci sono delle criticità che noi stessi abbiamo evidenziato, cercheremo adesso, con alcuni emendamenti governativi, di porre dei rimedi; perché l'ultima cosa che vogliamo è che il personale sia posto in una condizione di incertezza per un verso, ma anche che il direttore del DIS debba assumersi delle responsabilità che non gli sono proprie. Siccome c'è anche un tema di assunzione di responsabilità,

vedrete, tra le altre cose, che noi vorremmo dare inizio a tutta l'attività con la nomina del direttore della nuova Agenzia. Non con la conversione in legge del decreto, perché si rischierebbe di avere un lasso di tempo, anche di pochi giorni, che potrebbe compromettere quell'esigenza a cui facevo riferimento prima, cioè che non ci siano soluzioni di continuità.

Sul *cloud* ho risposto. Per quanto riguarda la *SolarWinds* noi abbiamo già relazionato al Copasir, chi mi ha preceduto ha relazionato al Copasir. Vi posso dire che anche in quella vicenda ci sono molte enunciazioni e poche certezze, perché su di essa molto spesso si tira la giacca da una parte e dall'altra. È ovvio che incerta può essere la matrice, assolutamente certi sono i danni che sono stati prodotti. Credo che, più che attardarci sulla natura della minaccia, dovremmo sempre più concentrarci sugli esiti che la minaccia produce. È il motivo per il quale la realizzazione di un'agenzia di questo tipo rappresenta, almeno nelle intenzioni del Governo e, più modestamente, di chi vi parla, un'esigenza primaria.

PRESIDENTE. Ringrazio il sottosegretario Gabrielli e dichiaro conclusa l'audizione.

La seduta termina alle 16.05.

Licenziato per la stampa
il 4 agosto 2022

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

18STC0195300