COMMISSIONE IX
TRASPORTI, POSTE E TELECOMUNICAZIONI

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

14.

SEDUTA DI MERCOLEDÌ 12 GIUGNO 2019

PRESIDENZA DEL PRESIDENTE **ALESSANDRO MORELLI**

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; Liberi e Uguali: LeU; Misto: Misto; Misto-Civica Popolare-AP-PSI-Area Civica: Misto-CP-A-PS-A; Misto-Minoranze Linguistiche: Misto-Min.Ling.; Misto-Noi con l'Italia-USEI: Misto-NcI-USEI; Misto-+Europa-Centro Democratico: Misto-+E-CD; Misto-MAIE - Movimento Associativo Italiani all'Estero: Misto-MAIE; Misto-Sogno Italia - 10 Volte Meglio: Misto-SI-10VM.

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE ALESSANDRO MORELLI

La seduta comincia alle 14.50.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata, oltre che mediante il resoconto stenografico, anche attraverso la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla *web-TV* della Camera dei deputati.

Audizione del direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulle nuove tecnologie delle telecomunicazioni, con particolare riguardo alla transizione verso il 5G e alla gestione dei *big data*, l'audizione del direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri.

Ringrazio il prefetto Gennaro Vecchione, direttore generale del DIS, per aver accettato l'invito della Commissione e gli cedo la parola per lo svolgimento della sua relazione.

GENNARO VECCHIONE, *direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri*. Signor presidente, onorevoli componenti di questa Commissione, sono qui insieme al vicedirettore vicario e al vicedirettore generale, Enrico Savio e il professor Roberto Baldoni, che mi assisteranno eventualmente nella fase in cui ci saranno le domande.

Ho accolto molto volentieri la richiesta di contribuire con un approfondimento specifico dalla peculiare prospettiva dell'*intelligence* nazionale a un'indagine conoscitiva sulla nuova tecnologia della comunicazione, che reputo davvero tempestiva e opportuna. Vi sono assai grato per questa possibilità di confronto in sede parlamentare e sono lieto di attenermi allo schema espositivo indicatomi, che suddivide l'indagine stessa in due aspetti distinti, l'uno riguardante gli sviluppi legati al 5G, l'altro relativo al tema dei cosiddetti « *big data* ».

Cominciamo, dunque, con il primo aspetto, il 5G, ma non senza evidenziare che le due tematiche sono comunque intimamente correlate, in quanto il 5G rileva, non solo sotto il profilo economico, ma prima ancora per le sue caratteristiche intrinseche di rete di nuova generazione.

È indubbio che, se entro il 2020 saranno connessi alla rete circa 50 miliardi di dispositivi *smart*, con un mercato potenziale di 12 trilioni di dollari entro il 2035, la possibilità di ottenere il primato nella diffusione di componenti, apparati e sistemi rappresenta al tempo stesso per ciascun attore in campo, sia esso operatore TELCO (*telecommunications company*), produttore di apparati di *network* oppure di dispositivi mobili, un'opportunità straordinaria di incrementare esponenzialmente il proprio fatturato e per i responsabili di *procurement* una sfida inedita e complessa, sulla quale mi soffermerò più avanti.

Nondimeno, in ragione del particolare *focus* di questa indagine conoscitiva, è utile prendere le mosse, non da questi risvolti economici, bensì dagli aspetti strettamente tecnici, che già di per sé configurano il 5G

come potenzialmente foriero di rischi dal punto di vista della sicurezza nazionale, rischi che vanno compresi e prevenuti, affinché si possano sfruttare appieno tutte le opportunità che il 5G offre per la crescita e lo sviluppo del Paese.

L'architettura del 5G crea delle partizioni di rete che condividono la medesima infrastruttura fisica di accesso e trasporto, il che configura tre categorie di *stakeholder*: i fornitori di tecnologia per l'infrastruttura, gli operatori mobili che si aggiudicano le frequenze e i soggetti terzi, i cosiddetti « inquilini », che mettono a disposizione dei loro clienti servizi digitali avanzati.

Un'architettura così complessa presenta rischi come accessi non autorizzati, vulnerabilità delle diversi partizioni di rete, intercettazione del traffico, possibili conflitti nella gestione della banda assegnata a ciascuna tipologia di traffico. Inoltre, il 5G, proprio tramite le sue soluzioni tecniche, basate per l'appunto sullo sfruttamento di elevate porzioni dello spettro elettromagnetico e anche sulla diffusione capillare di antenne e microcelle, di cui saremo invasi, promettendo estesa copertura della rete, grande velocità di trasferimento, elevato numero di connessioni simultanee a bassissima latenza, farà esplodere l'utilizzo dell'*internet of thing* e dei *big data* all'interno della società.

Il 5G è presupposto dell'*internet* delle cose (non possono esistere oggetti e servizi intelligenti senza uno scambio continuo e veloce di una grande quantità di informazioni) e sarà moltiplicatore di *big data*. Da qui l'estrema e intima connessione dei due aspetti che mi sono stati sottoposti. In altre parole, come vedremo meglio nella seconda parte di questo mio intervento, sarà in grado di veicolare un enorme e sempre crescente volume di dati, compresi i dati sensibili, la cui riservatezza, integrità e disponibilità vanno tutelate.

Vediamo ora in sintesi quali sono le minacce potenziali. Il pericolo deriva essenzialmente dal fatto che ben presto gli oggetti perennemente connessi a *internet* attraverso l'infrastruttura 5G e onnipresenti nelle nostre case e nei nostri uffici diventeranno possibili punti di accesso di minacce alla sicurezza nazionale.

Lo spiego con un esempio forse un po' pedestre, ma spero efficace. Pensiamo a una casa in cui aumentano le finestre e le porte di accesso, ognuna con un diverso meccanismo di chiusura da custodire e gestire e, allo stesso tempo, diminuisce la superficie dei muri. È evidente che quella casa sarà ancora più vulnerabile.

L'incremento nell'uso di dispositivi e componenti di *internet* delle cose incrementerà e implementerà le potenziali vulnerabilità delle infrastrutture di rete, ciò soprattutto se i produttori e i fornitori di questi dispositivi e servizi privilegeranno l'abbattimento dei costi rispetto alle funzionalità di sicurezza e se non verrà posto il giusto accento alle misure di sicurezza cibernetica e al controllo della catena di approvvigionamento.

Inoltre, la possibilità di avere macchinari, ad esempio industriali o biomedicali, e autoveicoli facilmente operabili via *internet* da uno *smartphone* apre la strada a possibili sabotaggi e attacchi *hacker*. Naturalmente la popolazione potrà beneficiare di servizi a maggior valore aggiunto, ma questo valore aggiunto deriva dal fatto che, raccogliendo enormi quantità di dati personali, avanzati algoritmi di intelligenza artificiale e di *machine learning* riescono a creare modelli e profili sempre più accurati e preziosi per gli individui: profili finanziari, medici, inclinazioni politiche, religiose, sessuali o peggio dati di autenticazione biometrici, il che fornisce vantaggio competitivo e potere a chi detiene queste informazioni e può sfruttarle per gli scopi più disparati.

Inoltre, non bisogna dimenticare che la potenza di questi strumenti, intesi come algoritmi capaci di generare ed estrarre dai dati nuova conoscenza, introduce delle problematiche di sicurezza, tanto nel mondo non classificato quanto e ancor più nel mondo classificato. Per questo è fondamentale tutelare quantomeno le informazioni classificate in tutte le fasi del processo di estrazione della conoscenza, a partire dai dati grezzi, attraverso le fasi di elabora-

zione e soprattutto nella fase di produzione del risultato finale.

Queste nuove tecnologie, nonostante abbiano avuto uno sviluppo relativamente recente e risultino in parte ancora in fase di prima applicazione, hanno già assunto un carattere di natura strategica, tale da indurre il legislatore a intervenire per dotare di adeguata disciplina il loro impiego e la loro messa in opera.

Peraltro, a riprova di quanto sia elevata e condivisa la sensibilità sul tema, lo scorso 26 marzo la Commissione europea ha pubblicato una raccomandazione in materia di sicurezza delle reti 5G rivolta agli Stati membri, nella quale, ferme restando le prerogative esclusive nazionali in materia di sicurezza e difesa, si prospetta l'adozione di un approccio concertato a livello di Unione europea, con la scadenza del 30 giugno imminente, per completare a livello nazionale una valutazione del rischio e rivedere metodi di gestione dello stesso e requisiti di sicurezza.

Al momento è sul tavolo una bozza di modello di *risk assessment* elaborata dall'Agenzia europea per la *cyber security* (ENISA), che sarà oggetto di analisi da parte del competente gruppo di cooperazione, cioè quello previsto dalla direttiva NIS (*Network and information security*), alla quale per l'Italia partecipa il punto di contatto unico inquadrato nel DIS e coordinato dai due vicedirettori che qui mi accompagnano.

Sul piano nazionale, in materia di 5G, con una recente novella alla cui stesura il DIS ha contribuito, contenuta nel decreto « Brexit », al decreto-legge n. 21 del 15 marzo 2012 è stato disposto, mediante l'introduzione del nuovo articolo 1-*bis*, un ampliamento della sfera di applicazione *ratione materia* della disciplina dei poteri speciali, volto a includere nel novero delle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale i servizi di comunicazione a banda larga basati sulla tecnologia 5G, in relazione ai quali trova applicazione il vaglio governativo previsto dall'articolo 1 del decreto-legge del 2012.

Merita in questa sede evocare due rilevanti profili applicativi della norma primaria del 2012. In primo luogo, le motivazioni che a suo tempo indussero il legislatore a modificare la disciplina dei poteri speciali prevista dal decreto-legge n. 332 del 1994 rimandavano all'esigenza di non legare più i poteri speciali in maniera esclusiva alla partecipazione azionaria pubblica, bensì di riferirli alle società pubbliche e private operanti in determinati settori e svolgenti attività di rilevanza strategica, non più genericamente operanti nei cosiddetti « servizi pubblici ».

È significativo al riguardo che la determinazione di non limitare nell'ambito della difesa, bensì di estendere espressamente ai macrosettori dell'energia, dei trasporti e delle comunicazioni gli *asset* suscettibili di costituire oggetto dell'esercizio dei poteri speciali da parte del Governo risalga già alla disciplina stabilita nel 1994.

In secondo luogo, è altrettanto significativo che siano i settori ad alta intensità tecnologica quelli da individuare ai fini della verifica della sussistenza di un pericolo per l'ordine e la sicurezza pubblica, a valle dell'estensione dell'ambito di applicazione dei poteri speciali intervenuta con le modifiche alla normativa del 2012 contenute nel collegato fiscale del 2017. Tutto ciò sta a significare che il disposto dell'articolo 1-*bis* è da iscriversi nel solco di un'evoluzione continua nella disciplina del *golden power*, dettata dai continui cambiamenti nel panorama della minaccia agli interessi nazionali essenziali del Paese.

Tanto premesso, ai sensi per l'appunto del nuovo articolo 1-*bis*, la stipula di contratti e accordi aventi a oggetto l'acquisto di beni e servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti inerenti i servizi di comunicazione a banda larga basati sulla tecnologia 5G, ovvero l'acquisizione di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione e gestione, sono soggetti alla notifica prevista dall'articolo 1 del decreto-legge n. 21 del 2012, al fine dell'eventuale esercizio del potere di veto o dell'imposizione, come spesso accade, di specifiche prescrizioni o condizioni.

Tale disciplina trova applicazione esclusivamente nei confronti di negozi giuridici aventi quale controparte un soggetto esterno all'Unione europea.

È peraltro doveroso segnalare a questa Commissione, sulla scorta di quanto ho appena evidenziato, che tale impianto normativo, essendo opportunamente intervenuto a disciplinare una materia di importanza nevralgica, vale a dire la sicurezza della catena di approvvigionamento nell'ambito della nuova tecnologia di telecomunicazione 5G, rimane a sua volta suscettibile di essere migliorato e completato con interventi integrativi, volti a conferire maggiore organicità alla disciplina e a definire un *corpus* normativo più coordinato.

Sono entrambe esigenze rilevanti, alla luce della *ratio* del sopracitato articolo 1-*bis*, che è quella di garantire i livelli massimi di sicurezza a protezione dei nostri dati e delle nostre infrastrutture strategiche, chiunque sia il fornitore di componenti, apparati e sistemi, tanto che la norma sul *procurement* qualificato nel 5G viene a porsi quale pilastro di un'architettura più ampia e articolata, finalizzata ad adattare l'ordinamento alle evoluzioni tecnologiche, nella misura in cui le stesse incidono sulla fisionomia della minaccia.

In tal senso, uno dei cardini del Piano nazionale per la sicurezza dello spazio cibernetico è l'avvenuta adozione da parte del Ministero dello sviluppo economico del decreto istitutivo del Centro di valutazione e certificazione nazionale (CVCN), a cui noi stiamo fornendo incondizionato supporto.

Questo, allorché operativo, controllerà tutti gli *asset* e i sistemi che verranno acquisiti per operare all'interno dei servizi essenziali per la sicurezza nazionale, non solo quelli della pubblica amministrazione. Si sta infatti lavorando per disegnare l'ambito di operatività di tale misura, con criteri di opportuno bilanciamento tra i princìpi di trasparenza e libero mercato e le esigenze di sicurezza nazionale.

Più precisamente, all'esito di quanto deliberato dal Comitato interministeriale per la sicurezza della Repubblica, organo fondamentale nel comparto dell'*intelligence*, il DIS ha elaborato una proposta che prevede l'istituzione di un perimetro di sicurezza nazionale cibernetica e che mira – importantissimo – a definire un sistema organico di misure e procedure di sicurezza a tutela di reti, sistemi e servizi informatici, da cui dipende l'esercizio di una funzione essenziale dello Stato.

Dall'inclusione nel perimetro deriverebbe l'obbligo per le amministrazioni pubbliche e gli operatori privati interessati di rispettare particolari misure di sicurezza, tra cui quella di sottoporre a specifico scrutinio tecnologico l'acquisizione di dotazioni di *information e communication technology* (ICT) destinate a operare sui predetti *asset* tutelati.

Oltretutto, nell'ambito delle attività volte all'innalzamento dei livelli di resilienza *cyber* del Paese, il Nucleo della sicurezza cibernetica, presieduto dal vicedirettore *cyber*, il professor Baldoni, su iniziativa del DIS che lo presiede, ha promosso l'avvio di un gruppo di lavoro chiamato a individuare possibili soluzioni tecnico-amministrative per garantire un approvvigionamento di beni e servizi informatici, caratterizzato da maggiori garanzie di sicurezza sotto il profilo cibernetico per la pubblica amministrazione.

Le attività del gruppo di lavoro si sono concluse con l'elaborazione di un testo unico di buone prassi e prescrizioni, sotto forma di linee guida obbligatorie dell'AGID (Agenzia per l'Italia digitale), pubblicate sul relativo sito *web* e in consultazione pubblica. Contengono misure di tipo organizzativo, funzionale e operativo, suddivise tra azioni da svolgere prima, durante e dopo la fase di *procurement*. Tali indicazioni sono obbligatorie per le forniture ritenute critiche dall'amministrazione committente, mentre vanno intese come semplici suggerimenti per le forniture non critiche.

È da segnalare che nell'ambito del gruppo di lavoro è emersa la necessità di provvedimenti legislativi per consentire di adeguare la normativa sugli appalti, in modo da equiparare la *cyber security* alla sicurezza sui luoghi di lavoro, così da poter evitare l'affidamento delle gare secondo il principio del massimo ribasso, prevedendo altresì la presenza di almeno un esperto di

sicurezza informatica nelle commissioni aggiudicatrici delle gare ICT.

Appare dunque chiaro che il *procurement* qualificato di soluzioni ICT, l'istituzione del CVCN, l'individuazione del perimetro di sicurezza allargato e l'aggiornamento delle norme sui poteri speciali sono quattro iniziative strettamente collegate tra loro sul piano operativo e concettuale.

In tale ottica è stato espressamente previsto nella norma del decreto-legge « Brexit », che ha novellato il decreto-legge del 2012, che, ai fini dell'esercizio eventuale del *golden power*, verranno valutati anche gli elementi sulla presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza tanto delle reti quanto dei dati che vi transitano.

Quattro pilastri, ma un'unica architettura nazionale di sicurezza cibernetica, al cui sviluppo il DIS, dopo aver contribuito attivamente alla stesura del decreto legislativo di recepimento della direttiva europea NIS (*Network and Information Security*), continua a fornire un forte impulso, assicurando la piena operatività del Nucleo per la sicurezza cibernetica e supportando il processo di digitalizzazione del Paese.

A proposito della normativa NIS è appropriato ricordare in questa sede, in relazione alle previste categorie di soggetti obbligati, vale a dire gli operatori dei servizi essenziali (OSE) e i fornitori di servizi digitali (FSD) che essa si pone in una condizione di neutralità tecnologica verso le soluzioni tecniche dagli stessi adottati. Tanto varrà evidentemente anche per i quattro settori del trasporto aereo, ferroviario, per vie d'acqua e su strada. Stante lo sviluppo tecnologico incessante, anche gli enti inclusi utilizzeranno tecnologie 5G e sempre più soluzioni *big data* per la loro operatività. Queste, a fronte della neutralità tecnologica della normativa NIS, saranno dunque oggetto di tutela e il DIS, alla luce delle funzioni che svolge a livello nazionale ed europeo quale punto di contatto unico, potrà possedere una visione d'insieme di tutte le tecnologie e dei sistemi informatici utilizzabili da OSE ed FSD.

Passo al secondo aspetto sul quale mi è stato chiesto di intervenire. Il tema dei *big data*, dalla prospettiva della sicurezza nazionale, comporta un duplice risvolto: bisogna analizzare come i *big data* possano essere utili per l'*intelligence* e allo stesso tempo occorre comprendere cosa l'*intelligence* possa fare per i *big data*.

Nondimeno, prima di addentrarmi nella problematica, desidero richiamare alcuni concetti che sono stati recentemente espressi dal Presidente del Consiglio e che rivestono una portata generale, poiché fissano taluni princìpi che valgono per tutta la pubblica amministrazione, nel cui contesto va dunque collocato anche questo duplice risvolto che ho appena menzionato, pur con le sue innumerevoli e sensibili specificità.

Il Presidente Conte ha in particolare sottolineato di recente che l'innovazione tecnologica deve riguardare anche il settore pubblico, che è il grande produttore e collettore di dati. I dati sono un pilastro essenziale in attività che sono sempre più interconnesse e che, pertanto, possono costituire uno strumento di non trascurabile rilievo per rendere sempre più rapida ed efficiente l'azione di governo. In sostanza, i dati sono un *asset* essenziale per l'esecutivo e serve un approccio strategico alla loro *governance*.

Se la tecnologia digitale è fondamentale per dare valore ai dati e se l'obiettivo finale è che i dati possano diventare la base del processo decisionale, strategico e operativo a tutti i livelli di governo, ne consegue che si rivelano comunque necessarie soluzioni tecnologiche che permettano di trasformare i dati grezzi in informazioni, quindi stabilendo relazioni in conoscenza, ossia in comprensione delle relazioni stesse.

In questo quadro, il Presidente del Consiglio ha opportunamente rammentato la centralità del problema delle garanzie. Quando parliamo di trattamento dei dati – lo sottolineo – qualunque trattamento, dobbiamo essere consapevoli che tale problema sussiste poiché sono sempre in gioco diritti fondamentali della persona, alla riservatezza, all'identità personale, all'onore, alla dignità, alla reputazione. Bisogna sempre vigilare affinché tutte le garanzie personali siano rispettate e io nella mia esperienza di comandante delle unità speciali

del Nucleo speciale *privacy* della Guardia di finanza ho maturato un'esperienza che conferma questa affermazione.

Anche in questo ambito va perseguito il bene comune, verso il quale devono convergere gli sforzi di tutti coloro i quali esercitano responsabilità pubbliche, dunque in modo particolare dell'*intelligence*, che è chiamata a operare nel più rigoroso rispetto del perimetro che la legge concede allo strumento non convenzionale, sicché intendo affrontare anche questo profilo.

Con queste premesse, veniamo ora allo scenario dei *big data*, che rimanda a un concetto familiare ai nativi digitali, secondo i quali, se una cosa non si trova su *internet*, allora non esiste. La conseguenza è che sta nascendo una nuova coscienza collettiva dove la propria esistenza, per essere tale, deve essere certificata dalla rete. È un processo inevitabile, già cominciato da qualche anno, che sta lentamente ma inesorabilmente modificando la geografia del mondo e della società sinora conosciuta. Pertanto, nei prossimi anni la rete non andrà a occupare semplici spazi in cui oggi non è presente, ma ne sarà la base permanente e portante.

All'origine di questo processo evolutivo vi è per l'appunto la crescita del concetto di *big data*, ovvero di enormi quantità di dati generati da un numero incalcolabile di sorgenti. L'idea è la cosiddetta « regola delle tre V » (volume, varietà e velocità di aggiornamento), che ultimamente si è evoluta nelle quattro « V », con l'aggiunta della veridicità e addirittura nelle 5 « V », tenuto conto – non va mai dimenticato – che le quattro caratteristiche prese assieme ne generano una quinta, cioè il valore, in altri termini il profitto.

Ciò comporta la necessità di strutturare nuovi sistemi di *data storage* inseriti in enormi *data center*, in grado di gestire quantità innumerevoli di informazioni a velocità elevatissima. L'elaborazione di tali volumi di dati viene ripartita in modo omogeneo tra il *data center* al centro e l'*internet* delle cose in periferia, come una sorta di enorme organismo vivente perennemente connesso ad alta velocità.

Grazie all'impatto delle tecnologie *wireless* e alla diffusione di prodotti intelligenti, il volume mondiale dei dati sta crescendo in maniera impressionante. Si prevede che entro il 2025 la sfera dei dati globali aumenterà fino a 163 miliardi di *Z-byte*, ossia dieci volte di più dei dati che esistevano soltanto tre anni fa. Più di un quarto di questi dati sarà in tempo reale e questo quarto sarà costituito per il 95 per cento da dati riconducibili all'*internet* delle cose.

Se tutto e tutti saranno connessi, i dati digitali diventeranno un bene essenziale da preservare. Infatti, gli oggetti intelligenti faranno sì che molti componenti umani saranno codificati in metadati e successivamente trasformati in *bit*. I metadati acquisiranno, quindi, un valore assoluto nel nuovo universo digitale.

Pertanto, il nuovo obiettivo dell'*intelligence*, ma anche delle forze e degli attori che essa contrasta innanzitutto sul terreno della prevenzione, sarà verosimilmente rappresentato dai dati digitali. I dati muoveranno ogni settore della società. Chi disporrà dei dati avrà la conoscenza e quindi, in teoria, il controllo.

La nuova generazione di tecnologie e architetture di *big data* sarà progettata per catturare, identificare, estrarre e analizzare in modo economico informazioni di valore e grandi volumi di dati eterogenei. La crescita di questa specie di titano digitale influenzerà il mondo e non c'è dubbio che anche la capacità di fare *intelligence* sarà strettamente legata alla capacità di saper sfruttare questi dati.

In particolare, sul versante dell'analisi strategica, una delle attività più qualificanti che siamo chiamati a svolgere per elevare le informazioni a un livello superiore di conoscenza, il fatto che le persone siano sempre connesse con più dispositivi contemporaneamente, anche in modo inconsapevole, fornisce basi utilissime all'analisi di tendenze sociopolitiche, economiche e finanziarie.

È, però, importante coordinare e mettere a sistema le capacità e le competenze del DIS e delle agenzie operative AISE (Agenzia informazioni e sicurezza esterna) e AISI (Agenzia informazioni e sicurezza

interna) per un'analisi strategica unitaria di comparto. È in atto da parte nostra uno sforzo assiduo per integrare risorse umane e risorse tecnologiche, al fine di ottimizzare le nostre capacità previsionali.

Va scongiurato il rischio che, sebbene si disponga di ingenti moli di informazioni, tanto di origine umana quanto di natura tecnologica, i macro-fenomeni e i grandi *trend* evolutivi non vengano individuati e affrontati in tempo utile e in maniera adeguata e arrivino a spiazzarci. Nella dimensione operativa può rammentarsi a titolo di esempio che con la condivisione in rete di immagini e filmati ritraenti soggetti o situazioni della sfera personale vengano inconsapevolmente fornite numerose informazioni sensibili.

I *big data* rappresentano, quindi, un moltiplicatore significativo delle capacità di *intelligence* sia sul terreno informativo che su quello analitico, grazie all'introduzione di sofisticati algoritmi di codifica in grado di analizzare le immagini in tempo reale direttamente dai luoghi ove sono aggregate.

In questo contesto, le esigenze degli operatori dell'*intelligence* sono rappresentate da tre principali ambiti: l'ampliamento delle capacità di immagazzinamento delle informazioni acquisite; l'individuazione e lo sviluppo di algoritmi in grado di analizzare le informazioni contenute e le loro correlazioni; la formazione specializzata. È fondamentale che il patrimonio informativo raccolto sia tesaurizzato e reso fruibile per i nostri committenti istituzionali, ai quali di sicuro non devono essere riversati dati ingestibili per quantità e non certificati in qualità.

A tal proposito, siamo impegnati a costruire professionalità adeguate, una fra tutte quelle del *data scientist*. Una tale figura professionale è decisiva per immergersi in quel che poc'anzi definivo il « 4V ». Il *data scientist* è un esempio di professionista dotato della giusta *expertise* per il supporto all'*intelligence*. Parimenti, ci stiamo adoperando per formare operatori di *intelligence* capaci di interagire con i nativi digitali.

Quel che serve è promuovere una sempre maggiore integrazione tra TECHINT (*technical intelligence*) e HUMINT (*human intelligence*), ovvero tra le attività di raccolta ed elaborazione delle informazioni svolte mediante strumentazione tecnica e quelle svolte tramite contatti interpersonali. Allo stesso tempo, bisogna saper parlare lo stesso linguaggio dei nativi digitali.

Una ripercussione importante di tutto questo è che gli approvvigionamenti non possono e non devono essere orientati solo alla tecnologia, bensì all'integrazione uomo-macchina, così come è indispensabile costruire l'offerta formativa specialistica per le sfide del domani.

Come ho già riferito al Comitato parlamentare per la sicurezza della Repubblica, stiamo individuando nuove soluzioni organizzative per la scuola del sistema di informazione. I criteri sono ovviamente quelli di rigorosa economicità di gestione e di doverosa valorizzazione di quanto già esiste, ma anche di un orizzonte temporale ragionevole e commisurato all'obiettivo. La soluzione potrà essere quella di realizzare una struttura adeguata sotto il profilo logistico e residenziale e sotto quello delle dotazioni formative e addestrative, che riconosca alla scuola di formazione il ruolo di istituzione di alta formazione e ricerca sul modello di un'accademia.

In tale contesto, mi preme anche ricordare che disponiamo già di un vero e proprio volano culturale per l'evoluzione delle risorse verso l'innovazione. Mi riferisco a un tassello fondamentale dell'architetture sistemica e unitaria dell'*intelligence* nazionale, il Polo tecnologico di comparto. È un contenitore che permette di integrare, coordinare, sintetizzare e ottimizzare esperienze e risorse nel quadro di un partenariato fra *intelligence*, aziende e – sottolineo – università, tesa ad accelerare la ricerca secondo i migliori modelli occidentali, l'innovazione, come pure il trasferimento, la diffusione e la condivisione delle capacità *high tech* della nazione.

In quest'ultima analisi l'obiettivo di fondo è quello di potenziare l'abilità dell'*intelligence* nel ridurre l'incertezza sul futuro, rafforzando le capacità previsionali degli organismi, anche grazie all'analisi dei *big data*. Stiamo ammodernando il rapporto

tra uomo e tecnologia per incrementare quelle capacità logico-analitiche che ovviamente sono appannaggio esclusivo della risorsa umana, la quale, però, non può più considerarsi svincolata dall'interfaccia tecnologica.

La strada che stiamo percorrendo è quella del continuo aggiornamento professionale degli appartenenti al comparto e dei reclutamenti mirati ai migliori talenti nelle materie altamente specialistiche.

Lo scenario che ho appena tracciato implica parimenti alcune considerazioni afferenti all'esigenza di disporre di un quadro giuridico adeguato a supporto dell'attività di *intelligence*. Al di là di quanto generalmente noto in ordine al potenziamento dell'azione informativa in una cornice di legalità, attuato fra l'altro con i successivi interventi normativi occorsi tra il 2005 e il 2015 in materia di intercettazioni e controlli preventivi sulle comunicazioni, nonché con l'introduzione dell'istituto delle garanzie funzionali, grazie alla legge n. 124 del 2007, a emergere in connessione con la problematica dei *big data* sono soprattutto i profili legati alla tutela della *privacy*.

Ricordavo che ad essi il Presidente del Consiglio Conte si è richiamato recentemente e ciò è oggetto di costante stimolo nei confronti del comparto dell'*intelligence*. Vorrei a tal proposito attirare l'attenzione su un risvolto ben preciso dell'innovazione tecnologica, con una nota costruttiva fiduciosa nel futuro.

Tende ad attenuarsi sempre più la differenza tra dato personale e dato anonimo, mentre a generare valore è l'analisi aggregata e correlata dei dati, che ha un valore esponenziale, come è intuitivo. Caratteristica dei *big data* è che ciascun dato può essere ricondotto a un profilo di persona piuttosto che a una persona individuata con nome e cognome, laddove i gestori dei dati stessi si moltiplicano all'infinito.

Ne derivano conseguenze importanti sul piano giuridico, poiché questo mette in discussione la nozione stessa del titolare del trattamento, ma a fronte di ciò il Regolamento europeo sulla tutela dei dati personali, entrato in vigore dopo due anni di latenza ormai da un anno (il 24 maggio dell'anno scorso) impone che taluni princìpi vengano applicati in maniera uniforme, concreta e sistemica su tutto il territorio dell'Unione europea. Questa era un'esigenza che anche sotto il profilo operativo avvertivo, in quanto rilevavo il differente atteggiamento nei confronti di questo tema, configurando un deciso salto di qualità giuridico e per certi versi anche culturale.

Desidero al riguardo richiamare quanto opportunamente osservato dall'attuale presidente dell'Autorità garante per la protezione dei dati personali, il professor Antonello Soro, in ordine a una delle caratteristiche fondamentali del regolamento, che valorizza la dimensione dinamica del dato personale, nella consapevolezza di come le potenzialità del *big data analytics* di estrarre informazioni che ci riguardano anche da semplici frammenti privi di correlazioni tra loro aumenti a dismisura le possibilità di reidentificazione anche di dati in apparenza anonimi.

In particolare, anche nella valutazione dell'Autorità garante nazionale, il regolamento europeo contiene talune norme e garanzie di particolare interesse per i trattamenti su larga scala quali quelli realizzati sui *big data*. Infatti, il regolamento è applicabile anche a trattamenti svolti da imprese situate all'estero, ma i cui servizi siano destinati o profilino persone che si trovano nell'Unione europea; prevede precise garanzie rispetto ai processi decisionali automatizzati, che esigono, almeno in ultima istanza, il filtro dell'uomo; introduce misure che mirano a iscrivere direttamente nei sistemi e nei dispositivi le tutele per l'interessato; realizza un ragionevole equilibrio tra le esigenze di utilizzo dei dati su larga scala per fini di utilità sociale con il diritto degli interessati alla protezione delle informazioni che li riguardano; descrive il sistema sanzionatorio, adottando tra l'altro il criterio della proporzionalità della sanzione pecuniaria al fatturato.

Mi preme evidenziare che, anche alla luce di tali importanti innovazioni, all'inizio del mio incarico sei mesi fa e nell'imminenza della scadenza del protocollo d'intenti tra il Dipartimento e l'Autorità garante, ho tenuto a promuovere, con la

piena e convinta adesione della controparte, non un semplice rinnovo, ma un vero e proprio rifacimento e rilancio dell'accordo.

Infatti, la nuova intesa istituzionale sottoscritta il 6 marzo scorso è stata revisionata nel suo contenuto, ora adeguato al regolamento europeo, oltre che alla direttiva *law enforcement* e, dunque, rafforzato ed esteso: è stata inserita nel quadro della nuova disciplina vigente sia in materia di protezione dei dati personali che di sicurezza cibernetica, nella misura in cui prevede interlocuzioni privilegiate – questo è molto importante – per la condivisione delle notifiche di violazione dei dati personali che ricadono nel regolamento europeo, a vantaggio del nucleo per la sicurezza cibernetica.

Si tratta di un significativo patrimonio di informazioni rilevanti per il comparto. Basti considerare che soltanto negli ultimi sette mesi dell'anno scorso sono giunte all'autorità ben 630 notifiche di *data breach*, che hanno riguardato come titolari del trattamento soggetti pubblici (27 per cento dei casi) e soggetti privati (73 per cento). In sostanza la cooperazione tra Autorità garante e organismi è stata potenziata, sino a porsi come una seconda opportunità per una migliore *governance* digitale, a dimostrazione che quest'ultima è viabile, così com'è possibile, elevando il livello della collaborazione istituzionale con sinergie concrete volte a incoraggiare i problemi posti dall'innovazione tecnologica, realizzare un bilanciamento fruttuoso tra tutela della *privacy* e presidio della sicurezza nazionale.

Mi avvio alla conclusione. Ho parlato di costruttiva fiducia nel futuro, adducendo esempi tangibili vuoi sul versante 5G vuoi sul versante *big data*, poiché sono convinto che le criticità, per quanto complesse, siano comunque gestibili, a condizione, però, che vengano affrontate, oltre che con linee di azione concrete, con l'abito mentale appropriato, con un elevato livello di sinergie istituzionali senza confusioni e con grande chiarezza di attribuzione di responsabilità e sulla base di una cognizione profonda delle diverse implicazioni della rivoluzione tecnologica, nonché intervenendo, laddove necessario, con le opportune iniziative legislative.

In ultima analisi, l'*intelligence* è direttamente chiamata in causa dalla vera e propria rivoluzione nel modo di percepire, elaborare e diffondere la conoscenza nel mondo che è stata determinata dalle innovazioni *cyber* e di *information and communication technology*. La società sarà sempre più permeata dalla dimensione digitale; sempre più il cyberspazio sarà precondizione ineludibile per la crescita economica e sociale, per il monitoraggio e la gestione delle infrastrutture critiche e strategiche, per l'esercizio dell'azione di governo. Quanto più i sistemi diverranno complessi, tanto più saranno vulnerabili.

Le nuove tecnologie amplificano le capacità operative del comparto, che è deciso ad avvalersene, ma parimenti continuerà convintamente a investire molto anche sul fattore umano. Sarà sempre quest'ultimo, non la tecnologia in sé, che rimane solo uno strumento, a fare la differenza, a individuare moduli operativi, linee di intervento, proposte e soluzioni atte a farci trovare sempre un passo oltre gli attori e fattori ostili (e ce ne sono).

Vi sono due paletti ben precisi. Il primo paletto è che il sistema d'informazione per la sicurezza della Repubblica operi a protezione degli interessi nazionali esclusivamente nel rispetto di leggi, indirizzi, obiettivi e finalità generali deliberate dal Comitato interministeriale per la sicurezza della Repubblica. Questo è l'unico mandato al quale siamo e restiamo votati.

Il secondo paletto è che le criticità con cui dobbiamo misurarci postulano che si agisca lungo tre direttrici: la stima precoce della minaccia, che è il compito primario dell'*intelligence*, la sicurezza dell'ecosistema dell'informazione e la consapevolezza del rischio che non possono essere percorsi, se non con l'ascolto attivo e con l'ingaggio responsabile di tutti i componenti del sistema Paese.

In tal senso, ci avviamo a fare un'attività di sensibilizzazione a livello nazionale nei confronti di tutto il sistema economico per la prima volta, aggiungendola a quell'attività di sensibilizzazione che stiamo condu-

cendo presso tutto il sistema informativo, a cominciare dall'università e a cominciare dai soggetti obbligati dalla direttiva NIS, cioè operatori dei servizi digitali e fornitori dei servizi digitali, che ricordavo prima, ma senza che ci si limiti a essi, ma piuttosto coinvolgendo anche il tessuto produttivo, l'accademia, i centri di ricerca, la società civile e l'opinione pubblica.

In conclusione, la quinta rivoluzione ICT non richiede all'*intelligence* di stravolgere la sua fisionomia istituzionale moderna, costruita nei dodici anni di applicazione della legge di riforma, al contrario la corrobora in uno dei suoi connotati più distintivi: la flessibilità e l'adattabilità al cambiamento. È questa in estrema sintesi la linea di pensiero che tenevo a condividere in quest'Aula. Vi ringrazio per l'attenzione.

PRESIDENTE. Grazie a lei, prefetto.

Do la parola ai colleghi che intendano intervenire per porre quesiti o formulare osservazioni.

FEDERICA ZANELLA. Grazie mille, direttore. È stato molto chiaro e ha toccato tantissimi temi interessanti, quindi io cerco di analizzarne alcuni, poi credo che i colleghi approfondiranno altri aspetti.

Sicuramente lei ha messo in luce qualcosa che è emerso in quasi tutte le nostre audizioni sul 5G, ovvero il fatto che la moltiplicazione di dati e di possibili punti di accesso crea dei *vulnera* per la sicurezza nazionale, ma anche per la nostra *privacy*.

Noi sappiamo che oggi il possesso e lo sfruttamento dei dati sono la nuova posta in palio per la sovranità, quindi anche in questo senso vi riguarda e non è un caso che tra Cina e Stati Uniti si stia giocando una battaglia, non solo commerciale evidentemente, sotto questo profilo.

La prima cosa che le vorrei chiedere è proprio questa. Lei ha parlato della possibilità dell'utilizzo del potere di veto anche per quanto riguarda gli aspetti di forniture, infrastrutture, eccetera. Qualche settimana fa *Bloomberg* ha evidenziato come sia emersa dal 2011 una problematica per quanto concerne le infrastrutture Huawei, denunciata da Vodafone, su delle *back doors* sconosciute, attraverso le quali, in infrastrutture strategiche, potevano essere stati estratti dei dati anche molto sensibili. Questo problema ha riguardato, non solo l'Italia, ma anche la Spagna, il Portogallo, la Germania e in parte gli Stati Uniti.

La prima domanda è questa. Trump negli Stati Uniti sta combattendo una battaglia non indifferente contro Huawei. Voi avete parlato della possibilità di porre un veto e di stabilire quali possono essere le forniture critiche e quelle non critiche, però il nostro Governo ha creato un memorandum di intesa, primo in Europa, proprio con la Cina. Sotto questo profilo potrebbero esserci delle criticità ? Questa ovviamente è la prima domanda.

La seconda è un po' più semplice. Lei faceva riferimento a un *corpus* normativo suscettibile di essere migliorato. Quali sono, vista la vostra esperienza in materia, le possibilità di miglioramento in questo senso ? Il GDPR (*General data protection regulation*) ha aiutato. Noi lo abbiamo seguito, perché siamo stati noi a sollecitare il fatto che ci fosse un recepimento veloce e fosse esaminato dalla Commissione speciale, perché l'anno scorso non erano ancora insediate le Commissioni, quindi lo conosciamo abbastanza bene. Non risolve tutti i problemi di *privacy*.

Vogliamo sapere, considerata la sua grande competenza, se ha qualche suggerimento da darci, visto che siamo chiamati a svolgere il ruolo di legislatori.

VINCENZA BRUNO BOSSIO. Grazie per la presentazione. Naturalmente, dovremo rileggercela, anche perché sono stati citati molti riferimenti normativi. Certamente conviene rileggere la sua relazione con attenzione.

Naturalmente, a quest'indagine conoscitiva sono già intervenuti diversi soggetti e ognuno in qualche misura deve fare la sua parte in questa rivoluzione digitale, che non è più la quarta, evidentemente, ma forse la quinta, la sesta.

Di una cosa siamo sicuri: se si mette insieme intelligenza artificiale e *big data*, che vengono esponenzialmente aumentati o comunque fatti circolare dal 5G, c'è sicuramente una grande opportunità per le

imprese, come una grande opportunità di lavoro per i giovani, a patto che si sviluppino le competenze digitali. Nello stesso tempo, insieme alle opportunità, come in tutte le rivoluzioni industriali, anche la prima, aumentano i rischi, e quindi c'è un problema che riguarda il legislatore, su cui evidentemente siamo ancora molto in ritardo, perché si deve definire meglio la connotazione di questi rischi e chi è preposto alla sicurezza nazionale, e in questo momento più che mai alla sicurezza cibernetica.

Ora, io vorrei sottolineare, forse perché dalla presentazione non è emerso con nettezza, e ci tengo invece a sottolinearlo, che il DIS è il punto di contatto unico in base anche all'attuazione della direttiva NIS. Voi siete, quindi, lo snodo fondamentale della sicurezza cibernetica in Italia anche in rapporto all'Unione europea.

A questo proposito, vorrei capire a che punto è la costituzione del CSIRT, il *Computer Security Incident Response Team*, che dovrebbe unificare i due CERT *(Computer Emergency Response Team*) nazionali e che è sempre stato un obiettivo fondamentale fin dal tempo del primo piano per la sicurezza cibernetica, il famoso decreto del gennaio 2013, per quel che riguarda l'identificazione degli operatori di servizi essenziali. Penso che sia importante capirlo, almeno per quel che ci riguarda, per quel che mi riguarda.

Io credo che il modo migliore per evitare che la rivoluzione digitale diventi una preoccupazione piuttosto che essere vissuta come un'opportunità – considerato che, preoccupazione o opportunità, come lei stesso ha detto, ormai l'esistenza di ognuno di noi coincide con la rete e anche con l'intelligenza artificiale (questi telefonini sono pieni di intelligenza artificiale) – sia quello di pensare sicuramente a un'educazione in questa direzione, soprattutto per il singolo e per le imprese.

Il GDPR, sostanzialmente, impone una responsabilità al produttore dei dati. Nello stesso tempo, però, dobbiamo sentirci le spalle coperte dal vostro ruolo di tutela.

GIORGIO MULÈ. A integrazione di quanto già detto dalle colleghe deputate, ringrazio il direttore generale Vecchione per una relazione che è stata esaustiva nei contenuti, ma coraggiosa – mi consenta – nella sua chiarezza per il fatto di non nascondere nulla, bensì di mettere sul tappeto lo scenario davanti al quale ci troviamo.

Lei ha molto insistito sulle minacce potenziali e sulla valutazione del rischio. Quello che mi interessa sapere meglio riguarda quella che lei individua come creazione del perimetro, che io traduco volgarmente in una fortezza da costruire per proteggerci. Lei individua quattro pilastri, quattro iniziative, che sono o dovrebbero essere una precondizione all'ingresso di una tecnologia così innervante nel tessuto sociale.

La domanda è: ritiene che questo perimetro debba appunto essere pretermesso all'ingresso della tecnologia ? I tempi che lei individua ci consentono di poterlo fare ?

DAVIDE GARIGLIO. Ringrazio il direttore generale e i vicedirettori per la loro presenza e per il loro contributo.

Ovviamente, il vostro ruolo e i temi principali di cui siete responsabili hanno portato anche in questa sede a sfiorare, a trattare temi che attengono alla vera e propria sicurezza nazionale, temi che potremmo definire di difesa vera e propria del nostro Paese, della nostra comunità, ma non è su questi che credo dobbiamo qua attenerci, perché già esiste un'apposito organo parlamentare, il COPASIR (Comitato parlamentare per la sicurezza della Repubblica), deputato ad affrontare queste tematiche.

Va da sé, invece, che il tema della difesa dell'individuo, dell'impresa, della libertà individuale, come tutelate dalla Costituzione, è un problema che il 5G pone esponenzialmente. Il fatto che si vedano in vendita su Amazon e su altri siti, sempre a prezzi ormai di saldo, prodotti per l'*Internet* delle cose, per dialogare con le cose, dialogare con la rete e da collocare in qualsiasi camera, dà l'idea di quanto potenzialmente invasiva sia l'intrusione che questi mezzi di comunicazione hanno sulla nostra vita, sulla vita delle nostre imprese, e quindi anche sulla competitività delle nostre imprese.

Per questo faccio mia la domanda che è stata già posta dalla collega Zanella. Poiché stiamo occupandoci, ed è competenza della nostra commissione, sul tema delle telecomunicazioni, del passaggio al 5G e di come il 5G eventualmente cambierà le vite dei nostri concittadini, il problema è questo: la normativa che abbiamo è adeguata a vostro parere o occorre prevedere ulteriori interventi di tipo normativo ?

Più volte, avete fatto riferimento a eventuali evoluzioni normative, eventuali interventi normativi. Lasciando perdere ciò che non è di competenza nostra, che attiene a un problema di difesa strategica, il nostro impianto normativo, a cominciare dall'attuazione delle direttive dell'Unione europea, offre una strumentazione adatta dalla nostra visuale di tecnici ed esperti per raggiungere l'obiettivo e per dare la massima garanzia di libertà individuale alla persona e all'impresa ?

Soprattutto, quanto è da implementare il sistema di formazione degli individui ? Se, infatti, mandiamo qualsiasi soldato al fronte, questo può essere dotato di una norma sofisticata, ma se non la sa usare, non gli giova. E, anzi, più l'arma è sofisticata e più l'addestramento è importante.

Qui abbiamo, non soldati che vanno in guerra, ma persone che sono inconsapevoli di avere addosso degli strumenti di intrusione e che devono essere formati. Specie su questo, come è stato detto, credo che nel nostro Paese ci sia un *gap* di informazione e di conoscenza rispetto ad altri Paesi occidentali su cui questa Commissione, invece, un ruolo potrebbe averlo.

Vi sarò grato quindi per i vostri suggerimenti.

PRESIDENTE. Desidero anch'io porre due domande rapidissime, di carattere tecnico.

Durante quest'indagine conoscitiva, abbiamo sentito più volte citare il termine « anonimizzazione ». Come, però, è stato sottolineato, a volte ci può essere un pericolo: l'anonimizzazione viene realizzata, ma poi si può – uso un termine assolutamente improprio, ma assolutamente comprensibile, altrettanto comprensibile – tornare indietro rispetto all'anonimizzazione.

La seconda questione è se esista, nel vostro ambito, in un ambito legislativo, a me personalmente sconosciuto, una valorizzazione della *privacy* dei dati. Mi spiego.

Tutti potete sapere quando io compio gli anni senza andare all'anagrafe, ma andando su un *social media*. Probabilmente, il 90 per cento delle persone presenti ha inserito questo dato, chiaramente oltre, per chi è interessato, ai dati relativi alla propria appartenenza politica, a una serie di aspetti, e sono comunque dati rilevanti.

Noi, però, abbiamo scelto di concedere questi dati al pubblico, in quel caso, e all'azienda che mi concede il servizio del *social media*. Questo è un livello che noi abbiamo accettato.

Altro discorso è la cultura nell'affrontare anche la cessione dei dati.

Io ritengo che purtroppo la signora Maria, che decide di scaricare un'applicazione sul proprio cellulare cui sono allegate numerose pagine di condizioni e di informazioni, che vengono accettate senza particolare attenzione, non abbia esattamente idea, come noi peraltro, di che cosa sta cedendo al proprietario di quell'applicazione.

Esiste una serie di criteri in base ai quali i dati personali – faccio un esempio molto pratico – data di nascita, luogo di residenza rientrano nella schedatura verde dei dati, mentre i dati sull'appartenenza politica e altro rientrano in quella gialla, e quindi poniamoci una domanda, e altri dati molto più sensibili rientrano nella sfera rossa ?

Questo riguarda le persone, logicamente, e quindi è l'esempio più semplice che si può fare, ma la problematica riguarda probabilmente anche i dati che vengono inserite in rete dalle aziende. Si tratta quindi, mancando una cultura digitale adeguata, di evitare che delle aziende rischino di cedere inconsapevolmente alcuni dati sensibili riguardo alle loro ricerche e al loro lavoro, che poi finiscono in rete e vengono utilizzati magari da aziende un po' più scaltre da questo punto di vista.

Esiste un criterio di valutazione del valore del dato, oggi ?

Do la parola al direttore generale Vecchione per la replica.

GENNARO VECCHIONE, *direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri*. Iniziamo con gli accordi dell'Italia con la Cina.

Noi abbiamo seguito direttamente questa fase di supporto all'azione governativa, e possiamo assicurare, almeno dal nostro punto di vista, che non si è mai trattato di un accordo politico né di messa in discussione dell'appartenenza alla NATO, all'Unione europea, all'OCSE e a tutte le organizzazioni occidentali.

Abbiamo traguardato tutti gli accordi commerciali sotto il profilo dell'*intelligence*, abbiamo proposto delle modifiche, che sono state accolte, in una riunione preparatoria presieduta dal Sottosegretario Giorgetti. Ci siamo assicurati che in sede di firma e sottoscrizione degli accordi si realizzassero queste misure minime di sicurezza.

Si è trattato di accordi commerciali, che non hanno un impatto sulla sicurezza nazionale, se non in alcuni profili marginali. L'unico accordo che può essere un po' più rilevante, ma ancora di più può servire, è quello del porto di Trieste.

Mi permetto di segnalare, in relazione alla vicenda del porto di Trieste, che qui si tratta semplicemente di scavare un po' di più per consentire al maggiore pescaggio del portacontainer di entrare nel porto di Trieste ed entrare direttamente in Europa.

La mia esperienza alla Presidenza del Consiglio, in un precedente incarico alle politiche europee, mi ha ricordato, banalmente, che i flussi di traffico producono dei diritti doganali: il 25 per cento viene trattenuto dal Paese di ingresso, ovviamente con tutto l'indotto (spedizionieri, turismo e altro).

Certamente, la deviazione del traffico con una settimana di crociera in meno delle portacontainer avrà un vantaggio per quelle provenienti da tutto il mondo, non solo dall'Estremo Oriente, ma chiaramente può aver provocato e provocherà una deviazione del flusso del traffico verso i porti del nord Europa. Questa, banalmente, potrebbe essere già una spiegazione di un certo livello di critiche nei confronti di quest'accordo, che ha natura logistica e si prefigge in sostanza lo scopo di rivitalizzare un porto che ha bisogno di una certo livello di traffico.

Per quanto riguarda il tema dei rapporti tra Stati Uniti e Cina, in particolare tra le aziende, con tutti i risvolti che stiamo vedendo (interruzioni, chiusure di aziende, sospensioni di convegni sino-statunitensi e così via) – stiamo assistendo a quest'attività di confronto tra questi due *player* internazionali – l'affermazione è sostanzialmente la seguente.

Il pericolo c'è anche oggi. Le intercettazioni si fanno anche oggi, come il monitoraggio e tutto il resto. Quanto alla deviazione della fibra ottica, l'80 per cento con uno *splitter* porta tutte le comunicazioni collegate ancora oggi, ancora oggi funziona così. Il 5G non farà altro che implementare quest'aspetto. Non si può quindi affermare che prima non ci fosse il pericolo, che fosse tutto a posto, con le fibre ottiche traguardate.

Se pensate soltanto ai punti di rigenerazione dei segnali mandati attraverso *internet*, e sono in posti penetrabili con una semplice chiave o addirittura con porte aperte, probabilmente il rischio c'è già adesso, ma in tutto il mondo, non solo in Italia. Questo già dovrebbe far ragionare, e far ragionare sul discorso della pericolosità che già esiste, è già insita nell'attuale sistema.

È ovvio che, tra la scelta di perdere un'opportunità per il Paese e quella di non respingere, ma di affrontare il problema come complesso, dividerlo in problemi più semplici e cercare di affrontarli uno alla volta, nel nostro Paese si è preferita la seconda soluzione.

Come è noto, la misura scelta, preannunciata in concomitanza con la firma di questi accordi, di questi rapporti con la Cina, in occasione della visita del Presidente cinese, è stata appunto quella di potenziare immediatamente quella norma che è già servita a coprire parte delle minacce palesi. C'è, infatti, un'altra grande parte di minaccia agli interessi economico finanziari del Paese che non è nota, ovviamente, ma lo è al COPASIR. Si cerca di

gestire la criticità, non respingendola, ma gestendo il problema.

Come si gestisce il problema ? Si gestisce utilizzando la norma del *Golden Power*: l'*intelligence* fornisce una parte fondamentale della sua attività con propri dirigenti e funzionari che partecipano alle attività presso la Presidenza del Consiglio.

La norma sul *Golden Power*, che riguardava soltanto la scalata delle società in certi posizionamenti strategici, con l'irrogazione di prescrizioni e di controlli è stata estesa, banalmente, all'acquisizione di tutti quei materiali, beni e altro che vanno a implementare la tecnologia 5G. Sostanzialmente, il 5G è stato equiparato a un tema di interesse nazionale, proprio perché è così che doveva essere trattato.

Come ci si è organizzati ?

Sapete meglio di me che una fase è già stata attuata con il Centro di Valutazione e Certificazione Nazionale (CVCN), a cui noi forniamo il massimo supporto, istituito presso il Ministero dello sviluppo economico, anche in termini di *software*, di *hardware* e di conoscenze tecniche di settore. Questa si completerà con la perimetrazione, come è stato già detto, del perimetro nazionale di sicurezza, questo fortino nel quale dovranno andare tutte le prescrizioni nei confronti dei soggetti che avranno titolo a essere inseriti con apposito decreto.

In questi giorni, in occasione della presentazione, proprio ieri, del decreto-legge « sicurezza-*bis* », si è ragionato dell'opportunità di completare il quadro normativo, in particolare con i Ministeri dell'interno e dello sviluppo economico, in sede di conversione del decreto. Stiamo lavorando. Nei prossimi giorni, si riunirà il *Computer Security Incident Response Team* (CSIRT) organismo tecnico da me presieduto e faremo il punto della situazione per completare il quadro di quest'attività.

Che cosa accadrà ?

Tutti coloro che vogliono acquisire tecnologie e materiali 5G, dovranno passare attraverso questo vaglio, dovranno notificarlo.

È chiaro che all'inizio questo fa tremare le gambe, pensando che tutti vogliono il 5G, e contemporaneamente, e che ci troveremo di fronte a una valanga, ma è soltanto una fase iniziale. Io credo che possiamo fare appello alla sensibilità delle imprese e di tutti, che all'inizio dovranno avere un po' di pazienza. Cercheremo di rispettare i tempi che sono stati assegnati dal legislatore, ma ci sarà bisogno di un confronto con le altre *intelligence*, tedesca, francese, inglese, che stanno maturando delle esperienze che ovviamente saranno oggetto di scambio.

Certamente, laddove il giudizio non sarà ostensibile, non lo potremo mettere nelle motivazioni di diniego, ma daremo la possibilità ai tecnici, attraverso il cosiddetto scrutinio tecnologico, di motivare l'eventuale modifica, o respingimento nei casi più importanti, dello scrutinio.

Per quanto riguarda Huawei, ma i soggetti extra Unione europea saranno tutti sottoposti a quest'analisi, questo ritengo sia un aspetto che sfugge a molti, molti citano i pezzi, il prodotto, la fibra. Il problema più grosso, invece, sarà quello di gestire la verifica dei prodotti venduti effettivamente. Io ho un modello depositato, ma non sono sicuro che quel modello, quando andrà in produzione, non verrà modificato. Serve, quindi, massima trasparenza.

Huawei non l'ha detto a noi, ma ha detto pubblicamente che loro sono disponibili. Ci mancherebbe che non fossero aperti alle nostre ispezioni e controlli, ovviamente casuali, per consentire appunto di verificare che il modello prodotto sia coincidente con quello depositato e approvato.

Per quanto riguarda il CSIRT, la questione non c'è. La legge ha già demandato alla Presidenza del Consiglio, a un dipartimento della Presidenza del Consiglio individuato nel DIS, che per legge ha la competenza nazionale nel settore della cyber-sicurezza, e quindi il CSIRT sarà assegnato, con il personale che è stato individuato numericamente, al DIS. Questa attribuzione verrà quindi fatta con un semplice decreto del Presidente del Consiglio.

È ovvio che questo, e cerco anche di rispondere in anticipo ad altre domande, sarà il sistema per superare definitivamente questi due poli CERT-PA e CERT-N, per riunirli e attribuire la responsabilità,

come ho detto nel corso dell'intervento, sottolineandolo, a un solo soggetto. Se si sbaglia, si sa chi è a risponderne, punto. Non ci devono essere dubbi.

VINCENZA BRUNO BOSSIO. I tempi ?

GENNARO VECCHIONE, *direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri*. Credo che basterà il DPCM. Non voglio spiazzare la Presidenza del Consiglio, il Ministro dell'interno e il Ministro dello sviluppo economico, ma ci stiamo lavorando ed è cosa pubblica e trasparente, e abbiamo ritenuto che in sede di conversione del decreto-legge « sicurezza-*bis* » possiamo introdurre il perimetro nazionale di sicurezza.

Completata quest'operazione, l'emendamento che stiamo preparando, se approvato dal Consiglio dei ministri e dal Parlamento, prevederà poi l'emanazione di decreti del Presidente del Consiglio dei ministri, tra cui l'attribuzione definitiva, come speriamo e auspichiamo, al DIS di questa funzione.

Per quanto riguarda gli identificativi degli OSE (Operatori di servizio essenziali), con il permesso del presidente lascerei brevemente la parola al professor Baldoni, perché è lui che ne ha seguito direttamente l'individuazione.

ROBERTO BALDONI, *vice direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri*. Per quanto riguarda gli OSE (operatori di servizio essenziali), essi sono stati identificati a fine gennaio, quindi abbiamo in Italia in questo momento 455 OSE identificati. Stiamo portando avanti, insieme alle cinque autorità – per chi non conoscesse la direttiva NIS, ci sono cinque autorità di riferimento, tra cui una è il Ministero delle infrastrutture – le linee guida di sicurezza cibernetica che dovranno essere adottate dagli OSE.

Siamo in fase di conclusione per quanto riguarda le linee guida. Dovremmo riuscire a farcela per la fine di giugno, il che significa che gli OSE a quel punto avranno quattro mesi per mettersi in regola, dopodiché partirà il discorso delle ispezioni.

Innanzitutto, ci tengo a dire che noi siamo nel gruppo di testa europeo per l'implementazione della NIS, insieme a Germania, Malta, ma lì la dimensione è diversa, e alla Gran Bretagna. Erano infatti quattro le nazioni che stavano nel gruppo di testa.

Ripeto, quindi: identificazione degli OSE è stata fatta, emissione delle linee guida, che per tre su cinque autorità – sono certo – avverrà entro la fine di giugno, mentre per le altre due, sanità e ambiente, che hanno la problematica di dover tenere conto anche dell'impatto regionale, avremo le linee guida, ma dovranno essere approvate anche dalla Conferenza Stato-Regioni, e questo vorrà dire un altro po' di tempo.

Ci tengo a dire un'altra cosa importante per quanto riguarda sempre l'identificazione degli OSE.

Abbiamo identificato 455 OSE. Questa non è un'operazione che finisce lì e che non rivedremo. È chiaro che, per far partire il sistema, di cui capite la complessità – dobbiamo coordinare cinque diverse autorità all'interno di cinque dicasteri differenti – abbiamo deciso di partire con un numero ragionevole ma nello stesso tempo maneggevole di OSE, e ci aspettiamo nel prossimo futuro, come previsto anche dalla direttiva NIS, una volta che la macchina è partita e riusciamo a gestire un certo *throughput*, a quel punto di poterli anche aumentare.

Ovviamente, il discorso del perimetro che il direttore prima ha sottolineato diverse volte per la sua importanza strategica è qualcosa che si colloca a un più alto livello rispetto al grado di maturità nella gestione del rischio *cyber* che dovranno avere le aziende che stanno dentro il perimetro rispetto a quelle che saranno nel perimetro NIS. Basti pensare che nel perimetro della sicurezza nazionale cibernetica abbiamo l'approvvigionamento qualificato, quello che ha ricordato il direttore. Ed è quella la differenza fondamentale tra chi sarà nel perimetro e chi sarà all'interno della direttiva NIS.

Passo ora agli altri due punti: innanzitutto come far arrivare i messaggi alle aziende.

Come ha ricordato il direttore, noi siamo impegnati in un *road show* che partirà a breve, in cui incontreremo le aziende, e uno dei punti importanti sarà proprio quello di iniziare a creare cultura su questo versante.

In secondo luogo, c'è un accordo AGID-Confindustria siglato alcuni mesi fa per un semplice motivo: le problematiche *cyber* non guardano pubblico e privato; è inutile far partire delle iniziative che vanno solo nel privato e altre che vanno nel pubblico. L'idea sul territorio è quella di unire le forze, e lo facciamo anche con le università, come il direttore ha sottolineato diverse volte, proprio per propagare quella cultura della sicurezza cibernetica che chiaramente è così importante per il nostro Paese, ma che, come tutti gli effetti culturali, ha bisogno di tempo per potersi diffondere.

GENNARO VECCHIONE, *direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri*. Questa è la parte che riguarda la necessaria operazione culturale. Per completare, vorrei condividere in questa sede anche quello che facciamo singolarmente, con le singole imprese, con il tavolo tecnico delle imprese. Sempre col permesso del presidente, lascerei la parola al vicedirettore vicario.

ENRICO SAVIO, *vice direttore generale vicario del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri*. Solo un dato: il tavolo tecnico imprese è uno strumento di interfaccia, di consultazione e di scambio con il sistema delle *corporate* infrastrutturali critiche e infrastrutturali *tout court* nazionali, siano esse fornitrici di beni e servizi di pubblica utilità, dall'energetico ai trasporti, siano esse fornitrici di sistemi industriali per la difesa o per la sicurezza.

Il tavolo tecnico imprese nasce cinque anni fa, quindi è un esercizio che ha costruito un rapporto fiduciario anzitempo con il mondo delle *corporate*, più semplice da interfacciare perché dotato di strutture e di competenze a livello macro, e quindi l'interlocuzione avviene più facilmente, tant'è vero che il *road show* sul territorio ha invece lo scopo di portare il messaggio alle piccole e medie imprese, da cui il nostro tessuto economico è composto prevalentemente, e tutta la filiera del subappalto che va anche verso le grandi *corporate* deve essere del pari sensibilizzata.

Il tavolo tecnico imprese scambia dati attraverso un sistema informatico, quindi sono collegamenti *on line*, ai sensi dell'articolo 13, comma 2, della legge n. 124 del 2007, che consente l'accesso alle banche dati, ad accesso controllato per l'appunto, mentre il comma 1 consente di instaurare rapporti di scambio con realtà pubbliche e private o a partecipazione pubblica attinenti a eventi, situazioni, incidenti di valenza cibernetica.

Da anni, quindi, abbiamo iniziato questo lavoro di osmosi con quel mondo. Riceviamo costantemente queste segnalazioni, che vengono analizzate attraverso tecniche evolute di *reverse engineering*, quindi proprio con un'analisi profonda dei *malware*, delle modalità di attacco, dei *pattern*, cioè dei *modus operandi* degli attaccanti, siano essi puntiformi, siano essi più strutturati, e restituiamo a queste realtà un *feedback*, un ritorno qualitativamente e scientificamente fondato sulla tipologia di minacce e sulle misure di riparazione del danno o di ristrutturazione dei sistemi.

Fino a oggi, ha funzionato. Adesso, la costruzione dell'architettura nazionale e del perimetro di sicurezza cibernetica trova già un motore acceso sottostante.

Ovviamente, tutto questo accade con modalità convenute con l'Autorità garante per la protezione dei dati personali, poiché noi abbiamo procedure di *log* e procedure di stoccaggio dei dati assolutamente accessibili al Garante e assolutamente tracciabili al fine di evitare ogni equivoco nella loro utilizzazione. Questo è lo strumento operativo già in essere e che non potrà che trovare ampliamento dal nuovo quadro normativo *in fieri*.

Per quanto riguarda l'anonimizzazione, è effettivamente – il tema è stato toccato nella relazione del direttore generale – un problema serio. Chi sta fuori ad attendere piccoli frammenti, ad attendere piccoli elementi e a riconnetterli in una logica, in senso lato, non strettamente tecnico, di ingegneria alla rovescia, quindi di ricostruzione di una profilazione partendo dal singolo dettaglio – si tratta di un lavoro vecchio come l'umanità, solo che adesso ha chiaramente delle caratteristiche digitali – sicuramente può giungere a profilare.

Si semplifica molto perché deriva da una banale operazione matematica: volume per velocità, cioè volume di dati per velocità di elaborazione. Ciò che l'intelligenza umana è in grado di fare rimane ancora in testa a tutti i processi costruiti dall'umanità, ma la macchina sta andando oltre nella capacità, cioè nella velocità di elaborazione del dato. Quando parliamo di 1.800.000 operazioni al secondo, parliamo di dati macro. Qui si può riuscire a riconnettere quei microscopici, infinitesimali elementi a un profilo e ricostruirne le tracce.

Il problema ha due facce: uno di prevenzione, l'altro di protezione, nella nostra visione.

Quello della prevenzione è stato già toccato. Significa accrescere la consapevolezza del cittadino, che deve prendere coscienza, tutti noi dobbiamo prendere coscienza di essere cittadini digitali, non solo cittadini. La digitalizzazione è un processo che coinvolge le nostre vite. È per questo che stiamo andando anche nelle scuole elementari, perché è lì che si comincia a creare la consapevolezza digitale.

In questo senso, non sarà sfuggita al Parlamento l'iniziativa che abbiamo lanciato due mesi fa: un videogioco su piattaforma Android e iOS, un *edutainment*, un *educational*, ma con funzionalità ludiche che servono ad attrarre l'interesse della fascia 11-13 anni, che serve, attraverso un gioco tipico di *scroll* – chi ne ha una conoscenza, sa di che cosa si parla – molto semplice, divertente e sfidante, a condurre attraverso dei passaggi di acquisizione di concetti, che cos'è un *trojan*, che cos'è un virus, che cos'è un *malware*.

VINCENZA BRUNO BOSSIO. Come si chiama l'*App* ?

ENRICO SAVIO, *vice direttore generale vicario del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri*. L'*App* è *Cybercity Chronicles*, ed è scaricabile gratuitamente. Non a caso, abbiamo fatto questo esercizio con il MIUR, con il Ministero dell'istruzione, che ha aperto le porte delle scuole da questo punto di vista.

Stiamo cercando di formare la prossima generazione dei nativi digitali in modo da farli dotare anche di certi strumenti, che non significa sovrapporsi a campagne di prevenzione e sicurezza. Si tratta proprio di consapevolezza di cittadinanza digitale, che è un altro tema. È l'esercizio libero di ciò che si vuole dire o pensare sapendo a che cosa si va incontro. Non vuol dire non fare questo, non fare quello. Significa sapere che cosa succede quando posti un tuo dato personale sui *social*. Poi tu fai la scelta di portarlo perché sei libero e sei digitale, però è consapevolezza, coscienza.

Dalla consapevolezza derivano il comportamento, possibilmente virtuoso, sempre nel ciclo della prevenzione, e il rapporto fiduciario che deve crescere con le istituzioni. A eventi criminosi o traumatici sono dedicate specifiche forze di polizia, ma c'è l'apertura ad un'osmosi, ad un dialogo che deve servire alle istituzioni preposte per monitorare e tracciare il fenomeno. Se l'evento non è riportato, l'evento non esiste, soprattutto sulla rete.

L'altra faccia della medaglia è quella della protezione.

Sulla protezione, sempre per quanto riguarda l'anonimizzazione e i dati e la privatezza dei dati, si sta facendo un grosso investimento di pensiero e di risorse relativo all'elaborazione anche di un algoritmo nazionale di cifratura. È necessario giungere a una capacità di protezione del dato che sia certificata e garantita da un'entità statale, e quindi devota all'interesse pubblico generale, cioè non lasciare solo alle soluzioni commerciali determinate necessità di protezione.

Ogni *provider* ha le sue doti, le sue capacità e fa i suoi investimenti positivi in termini di securizzazione del dato privato, e quindi

della sua anonimizzazione, ma l'istituzione pubblica deve garantire un livello di controllo indipendente nell'interesse generale.

Anche su questo c'è una dialettica che il collega Baldoni sta portando avanti a livello scientifico, evidentemente, perché si tratta di investire cuori, menti e risorse al fine di addivenire a uno strumento che consenta di proteggere quel dato.

GENNARO VECCHIONE, *direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri*. Credo che occorra completare la risposta alla domanda posta dal presidente sulle varie tipologie di dati.

ENRICO SAVIO, *vice direttore generale vicario del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri*. In parte, si ricollega a quello che diceva il vicedirettore generale vicario. È chiaro che c'è un problema nel momento stesso in cui le aziende rilasciano i propri dati, per esempio su *cloud*, mi veniva in mente mentre lei formulava la domanda.

È chiaro che, da una parte, non sono consapevoli del valore; dall'altra, possono non aver chiari i rischi che si corrono nell'inserire i dati all'interno di piattaforme che possono a loro volta essere « bucate », per cui a quel punto i dati vengono trafugati.

Da questo punto di vista, quello che stiamo facendo si colloca all'interno di un approccio generale per quanto riguarda, ad esempio, la realizzazione di un algoritmo di cifratura nazionale, che fa parte delle attività del piano operativo uscito nel 2017, come un elemento propedeutico, per poi realizzare un *cloud* di tipo nazionale.

Questo, ovviamente, ci permette, grazie anche alla cifratura a quel punto in nostro possesso, di dare un servizio ad alcune organizzazioni allo scopo di mettere i loro dati in luoghi sicuri.

Ovviamente, il problema è sempre una questione di consapevolezza rispetto alle aziende, al valore dei dati, a quello che rischiano nel mettere i dati all'esterno, con di contro la possibilità di aumentare il loro *business* facendo le stesse operazioni.

Quello che vogliamo cercare di portare all'interno del sistema è proprio di creare delle aree, delle piattaforme in cui è possibile portare l'informazione in una modalità, lasciatemi dire, più sicura. Ovviamente, chiunque lavora in questo settore sa perfettamente che la sicurezza completa non esiste, che gli attacchi sono sempre esistiti, esisteranno, cambieranno con la tecnologia, cambieranno con le modalità scelte dell'attaccante. Noi dobbiamo prepararci a questo scenario di mutazione continua.

Su questo, ahimè, come è stato già detto dal vicedirettore vicario, dobbiamo portare veramente avanti a livello culturale un discorso importante verso i cittadini e verso le imprese per far capire loro che siamo entrati in questa nuova era digitale, e che quindi siamo parte di questa trasformazione digitale e, come parte di questa trasformazione digitale, dobbiamo conoscere i meccanismi, avere delle conoscenze di base.

Faccio un esempio banale per far capire quanto sia importante che il cittadino entri in questa consapevolezza, l'impresa entri in questa consapevolezza. Abbiamo avuto un incidente importante, il 13-14 novembre, che ha portato all'attivazione dell'NSC (Nucleo di Sicurezza Cibernetica), e siamo risaliti fino al presidente, un incidente di sicurezza nazionale. Si è tradotto, da un punto di vista visibile verso l'esterno, nella chiusura dei tribunali nella giornata del 14 novembre.

All'interno delle attività di mitigazione e recupero di questa situazione, a un certo punto siamo dovuti uscire con una conferenza stampa, prima in assoluto, da parte di vertici dell'*intelligence*, ma perché ? Perché c'erano delle operazioni, come il cambio della *password*, che non potevamo imporre. E la cosa incredibile è stata che, fino a quando c'è stata la conferenza stampa, eravamo riusciti a raggiungere il 35 per cento delle *password* cambiate all'interno di un certo gestore di PEC di impiegati della pubblica amministrazione che era stato attaccato; venti ore dopo la conferenza stampa, eravamo arrivati all'87 per cento. Significa che abbiamo anche un retroterra culturale che ha capito l'importanza di quell'operazione.

È importante capire che i cittadini non sono fuori e le imprese non sono fuori da questa problematica, sono parte di questa

problematica, e tutti insieme dobbiamo agire, ognuno al suo livello di responsabilità.

GENNARO VECCHIONE, *direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri*. Per completare sulle altre domande che mi sono state fatte, un tema comune è quello della formazione, tema perfettamente centrato.

È una formazione, una consapevolezza, una *awareness* che non c'è. Quando mi sono insediato, c'è stato un altro incidente, un attacco a una società petrolifera nazionale all'estero: tre righe sul *Sole 24 Ore*, mentre la *Reuters* ha mandato lanci continui su quest'incidente. Qualcosa non andava, perché l'Italia non capiva e l'estero aveva capito che era un fatto grave.

Abbiamo chiamato l'amministratore, abbiamo capito che aveva comunicato al mercato perché, essendo una società quotata addirittura in borsa, aveva gli obblighi di informazione del mercato, ma poi c'è stato un problema perché non conosceva le regole di ingaggio, non sapeva con chi parlare, e questo non poteva succedere.

Come ha detto il collega, nei grandi gruppi il problema è già stato risolto, ma anche nelle grandi aziende isolatamente considerate questo aspetto va affrontato. Fino ad ora lo abbiamo solo spiegato. Manca però la consapevolezza. Bisogna fare una campagna di sensibilizzazione, che noi possiamo fare con i nostri fondi, con le nostre energie, con le nostre risorse, presso le aziende sul territorio. Manca la consapevolezza delle aziende, soprattutto, come ha detto il vicario, nelle piccole e medie aziende, che sono alla fine quelle che fanno lo scafo, quello che fanno il materiale d'armamento, e quindi devono essere monitorate. Già lo facciamo sotto il profilo del controllo con l'Ufficio centrale di segretezza per il rilascio delle attestazioni per lavorare materiali sensibili e strategici.

Quanto al perimetro di sicurezza, effettivamente, onorevole Mulè, sono assolutamente necessarie queste precondizioni, altrimenti ci esponiamo a un massacro il primo giorno che la rete si attiva.

Vi posso dire, dal momento che non rappresenta un argomento secretato, che è un problema che stiamo già affrontando: il 5G comporterà una serie di problematiche, di intercettazioni telefoniche, ambientali e così via, perché la velocità, il numero elevatissimo di antenne servirà a saltare passaggi che ci servono per poi produrre l'attività investigativa che ci interessa.

Questo sta portando a una sensibilizzazione del vertice politico e dei vertici della magistratura, che sono molto impegnati in questo momento. Se ci saranno delle cose da fare, veramente auspico che gli strumenti normativi che si renderanno necessari per consentirci, ma non solo a noi, bensì a livello europeo, di sviluppare attività investigative utilizzando la tecnologia, vengano adottati il più velocemente possibile. Non possiamo rimanere scoperti su temi delicati, come ad esempio quello del terrorismo. Auspico che ci sia una rapida valutazione, una volta individuate le criticità in questo settore.

PRESIDENTE. Ringrazio i nostri ospiti e tutti voi per la partecipazione.

Dichiaro conclusa l'audizione.

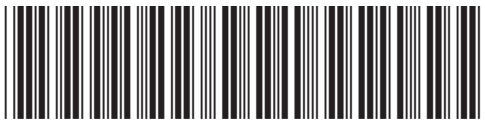
La seduta termina alle 16.20.

Licenziato per la stampa
il 13 novembre 2019

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

PAGINA BIANCA

PAGINA BIANCA



18STC0067050