AUDIZIONE DEL DIRETTORE GENERALE DEL DIS
PRESSO LA COMMISSIONE TRASPORTI DELLA CAMERA

INDAGINE CONOSCITIVA SU 5G E BIG DATA

Roma, 12 giugno 2019

Signor Presidente**,**
Onorevoli componenti di questa Commissione**,**

ho accolto molto volentieri la richiesta di contribuire, con un approfondimento specifico dalla peculiare prospettiva dell'intelligence nazionale, ad un'indagine conoscitiva sulle nuove tecnologie della comunicazione, che reputo davvero tempestiva ed 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 col 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.

  E' 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, produttore di apparati di network oppure di dispositivi mobili – una opportunità straordinaria di incrementare esponenzialmente il proprio fatturato;
  per i responsabili del 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 tecnologie per l'infrastruttura, gli operatori mobili che si aggiudicano le frequenze, ed 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 diverse partizioni di rete, intercettazione del traffico, possibili conflitti nella gestione della banda assegnata a ciascuna tipologia di traffico.
Non solo.
Il 5G, proprio tramite le sue soluzioni tecniche - basate, per l'appunto, sullo sfruttamento di elevate porzioni dello spettro elettromagnetico, ed anche sulla diffusione capillare di antenne e micro celle - promettendo estesa copertura della rete, grande velocità di trasferimento, elevato numero di connessioni simultanee e bassissima latenza, farà esplodere l'utilizzo dell'Internet of Things e dei Big Data all'interno della società.

Il 5G è presupposto dell'Internet of Things - 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, ossia, 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 ad Internet attraverso l'infrastruttura 5G, ed onnipresenti nelle nostre case e nei nostri uffici, diventeranno possibili punti di accesso di minacce alla sicurezza.
  Lo spiego con un esempio forse un po' pedestre ma spero efficace: pensiamo ad una casa in cui aumentano le finestre e le porte di accesso - ognuna con un diverso meccanismo di chiusura da custodire e gestire - ed allo stesso tempo diminuisce la superficie dei muri. E' evidente che quella casa sarà vulnerabile.

  L'incremento nell'uso di dispositivi e componenti di "internet delle cose" incrementerà 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) ed autoveicoli facilmente operabili via internet da uno smartphone apre la strada a possibili sabotaggi o 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 degli 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, ed ancor più, nel mondo classificato. Per questo è fondamentale tutelare quanto meno le informazioni classificate in tutte le fasi del processo di estrazione della conoscenza a partire dai dati grezzi, attraverso le fasi di elaborazione, e soprattutto nelle fasi 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 tali 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, con la scadenza del 30 giugno 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, al quale, per l'Italia, partecipa il "punto di contatto unico" inquadrato nel DIS.

- Sul piano nazionale, in materia di 5G, con una recente novella, alla cui stesura il DIS ha contribuito, contenuta nel Decreto Brexit[1], al Decreto Legge 15

[1] D.L. 25 marzo 2019 n.22

marzo 2012, n. 21[2], è stato disposto, mediante l'introduzione del nuovo art. 1-bis, un ampliamento della sfera di applicazione ratione materiae della disciplina dei poteri speciali, volto ad includere nel novero delle attività di rilevanza strategica per il sistema di difesa e di sicurezza nazionale i servizi di comunicazione a banda larga basati sulla tecnologia 5G, in relazione ai quali trova applicazione il vaglio governativo previsto dall'art. 1 del Decreto 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 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 settori dei servizi pubblici".
  Ed è significativo, al riguardo, che la determinazione di non limitare all'ambito "difesa", bensì di estendere espressamente ai macrosettori "energia, trasporti e comunicazioni" gli asset suscettibili di costituire oggetto dell'esercizio dei poteri speciali da parte del Governo risalga già alla disciplina stabilita nel 1994.

- e, 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, a significare che il disposto dell'art. 1-bis è da inscriversi nel solco di un'evoluzione continua della disciplina del Golden Power, dettata dai continui cambiamenti del panorama della minaccia agli interessi essenziali del Paese.

- Tanto premesso: ai sensi, per l'appunto, del nuovo art. 1-bis, la stipula di contratti o accordi aventi ad oggetto l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione ed 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 o gestione, sono soggetti alla notifica prevista

[2] In materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni. Convertito con modificazioni dalla legge 11 maggio 2012, n.56.

dall'art. 1 del D.L. 21/2012 al fine dell'eventuale esercizio del potere di veto o dell'imposizione di specifiche prescrizioni o condizioni.
Tale disciplina trova applicazione esclusivamente nei confronti di negozi giuridici aventi quale controparte un soggetto esterno all'Unione europea[3].

- E' 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
  ed a definire un corpus normativo più coordinato.

  Sono entrambe esigenze rilevanti,
  alla luce della ratio del sopracitato art. 1-bis, che è quella di garantire 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 ed 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 MISE del decreto istitutivo del Centro di Valutazione e Certificazione Nazionale, il CVCN.
  Questo, allorché operativo, controllerà gli asset e i sistemi che verranno acquisiti per operare all'interno dei servizi essenziali per la sicurezza nazionale: tutti, non solo quelli della Pubblica Amministrazione. Si sta infatti lavorando per disegnare l'ambito di operatività di tale misura, con criteri di opportuno bilanciamento fra i principi di trasparenza e libero mercato e le esigenze di sicurezza nazionale.

[3] Per tale intendendosi:

- ✓ qualsiasi persona fisica o giuridica che non abbia la residenza, la dimora abituale, la sede legale o dell'amministrazione ovvero il centro di attività principale in uno Stato membro dell'Unione europea o dello Spazio economico europeo o che non sia comunque ivi stabilito;
- ✓ qualsiasi persona giuridica interna all'Unione europea che risulti controllata direttamente o indirettamente da una persona fisica o giuridica esterna all'Unione europea;
- ✓ qualsiasi persona fisica o giuridica che abbia ottenuto i requisiti per poter essere considerata interna all'Unione europea al fine di eludere la normativa.

Più precisamente, ad esito di quanto deliberato dal Comitato Interministeriale per la Sicurezza della Repubblica, il DIS ha elaborato una proposta che prevede l'istituzione del perimetro di sicurezza nazionale cibernetica, e che mira 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 and Communication Technology" destinate ad operare sui predetti asset tutelati.

Oltretutto, nell'ambito delle attività volte all'innalzamento dei livelli di resilienza cyber del Paese, il Nucleo per la Sicurezza Cibernetica, su iniziativa del DIS che lo presiede, ha promosso l'avvio di un Gruppo di Lavoro chiamato ad 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". Pubblicate sul relativo sito web il 14 maggio, e in consultazione pubblica fino a domani, 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.
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 cybersecurity 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 di un perimetro di sicurezza allargato e l'aggiornamento delle norme sui poteri speciali sono quattro iniziative strettamente collegate fra loro sul piano operativo e concettuale. In tale ottica, è stato espressamente previsto, nella norma del Decreto 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 NIS, continua a fornire un forte impulso, assicurando la piena operatività del Nucleo per la Sicurezza Cibernetica e supportando il processo di digitalizzazione del Paese.

Ed a proposito della normativa NIS, è appropriato ricordare in questa sede, in relazione alle previste categorie di soggetti obbligati, vale a dire gli operatori di servizi essenziali (OSE) ed i fornitori di servizi digitali (FSD), che essa si pone in una condizione di neutralità tecnologica verso le soluzioni tecniche dagli stessi adottate. 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 in essi 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, ed 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 ed i sistemi informatici utilizzabili da OSE e FSD.

- Per quel che concerne il secondo aspetto che mi si chiede di approfondire, ossia il tema dei Big Data, dalla prospettiva della sicurezza nazionale comporta un duplice risvolto: bisogna analizzare come i Big Data possono essere utili per l'intelligence, ed allo stesso tempo occorre comprendere cosa l'intelligence può fare per i Big Data.

  Nondimeno, prima di addentrarmi nella problematica, desidero richiamare alcuni concetti che sono stati recentemente espressi dal Presidente del Consiglio[4], e che rivestono una portata generale, poiché fissano taluni principi 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 più 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 efficace 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 ed operativo a tutti i livelli di governo, ne consegue che si rivelano comunque necessarie soluzioni

[4] Intervento del Presidente Conte all'evento "Data Driven Innovation", presso il Dipartimento di Ingegneria dell'Università Roma Tre, 10 maggio 2019.

tecnologiche che permettano di trasformare i dati grezzi in “informazioni”, quindi stabilendo relazioni, ed 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 - sottolineo: “qualunque” trattamento - dobbiamo sempre 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.
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 anche dell’intelligence, anzi, in modo particolare dell’intelligence, che è chiamata ad 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 ad 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.
  E’ un processo inevitabile, già cominciato da qualche anno, che sta lentamente ma inesorabilmente modificando la geografia del mondo e della società sinora conosciuta, per cui nei prossimi anni la rete non andrà ad occupare semplicemente spazi in cui oggi non è presente, ma ne sarà la base 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 3V”, Volume, Varietà e Velocità di aggiornamento, che ultimamente si è evoluta nelle 4V, con l’aggiunta della Veridicità, o addirittura delle 5V, tenuto conto, e 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 centers, in grado di gestire Exabyte[5] di informazioni a velocità di Exaflop[6]. L’elaborazione di tali volumi di dati viene ripartita in modo omogeneo tra il data center al centro e l’internet delle cose (IoT) in periferia, come una sorta di enorme organismo vivente, perennemente connesso ad alta velocità.

[5] 1 Exabyte = 1 trilione di bytes
[6] 1 Exaflop corrisponde a 1018 operazioni al secondo

Grazie all'impatto delle tecnologie wireless e alla diffusione di prodotti "intelligenti", il volume mondiale dei dati sta crescendo in maniera impressionante. Si prevede[7] che entro il 2025 la sfera dati globale aumenterà fino a 163 miliardi di Zettabyte[8], 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% 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 comportamenti 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, sia dell'intelligence, ma anche delle forze e degli attori che essa contrasta anzitutto 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, della stessa.

La nuova generazione di tecnologie e architetture di Big Data sarà progettata per catturare, identificare, estrarre e analizzare, in modo economico, informazioni di valore da 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, cioè una delle attività più qualificanti che siamo chiamati a svolgere per elevare le "informazioni" al livello superiore della "conoscenza", il fatto che le persone siano sempre connesse, e con più dispositivi contemporaneamente, anche in modo inconsapevole, fornisce basi utilissime all'analisi di tendenze sociopolitiche, economiche e finanziarie.
  E' però importante coordinare e mettere a sistema le capacità e le competenze del DIS, dell'AISE e dell'AISI per un'Analisi Strategica unitaria, di Comparto. E' 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 macrofenomeni e i grandi trend evolutivi non vengano individuati ed affrontati in tempo utile ed in maniera adeguata, ed 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

[7] International Data Corporation, 2018
[8] 1 Zettabyte = 1 trilione di Gigabyte

della sfera personale, vengono inconsapevolmente fornite numerose informazioni sensibili.

I Big Data rappresenteranno quindi un moltiplicatore significativo delle capacità 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 per gli 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.
E' 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 quella del Data Scientist. Una tale figura professionale è decisiva per immergersi in quello 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.

Quello che serve è promuovere una sempre maggiore integrazione tra TECHINT e HUMINT, ovvero fra 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 quelli di rigorosa economicità di gestione, di doverosa valorizzazione di quanto già esiste, e di un orizzonte temporale ragionevole e commisurato all'obiettivo. La soluzione potrà essere quella di realizzare una struttura, adeguata sotto il profilo logistico-residenziale e sotto quello delle dotazioni formative ed 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 ad un tassello fondamentale dell'architettura sistemica ed unitaria della comunità intelligence nazionale: il Polo Tecnologico di Comparto. E' un contenitore che permette di integrare, coordinare, sintetizzare ed ottimizzare idee, esperienze e risorse nel quadro di un partenariato fra intelligence, aziende ed università teso ad accelerare la ricerca, l'innovazione, come pure il trasferimento, la diffusione e la condivisione delle capacità hi-tech nazionali.

In 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 fra 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 delle 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 fra il 2005 ed il 2015 in materia di intercettazioni e controlli preventivi sulle comunicazioni, nonché con l'introduzione dell'istituto delle garanzie funzionali grazie alla legge 124 del 2007 - ad emergere in connessione con la problematica dei Big Data sono soprattutto i profili legati alla tutela della privacy. Ricordavo che ad essi il Presidente Conte si è richiamato recentemente, e vorrei, a tal proposito, attirare l'attenzione su un risvolto ben preciso dell'innovazione tecnologica. Con una nota di costruttiva fiducia nel futuro.

  Tende ad attenuarsi sempre più la differenza fra dato personale e dato anonimo, mentre a generare valore è l'analisi aggregata e correlata dei dati. Caratteristica dei Big Data è che ciascun dato può essere ricondotto ad un "profilo di persona", piuttosto che ad 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 mette in discussione la nozione stessa di titolare del trattamento.

  Ma a fronte di tutto ciò, il GDPR, entrato in vigore il 24 maggio dello scorso anno, impone che taluni principi vengano applicati in maniera uniforme,

concreta e sistematica su tutto il territorio dell'Unione Europea, configurando un decisivo 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, Antonello Soro[9], in ordine ad una delle caratteristiche fondamentali del Regolamento, che "valorizza la dimensione dinamica del dato personale, nella consapevolezza di come le potenzialità della 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 GDPR contiene talune norme e garanzie di particolare interesse per i trattamenti su larga scala, quali quelli realizzati su Big Data. Difatti il Regolamento: è applicabile anche a trattamenti svolti da imprese situate all'estero, ma i cui servizi siano destinati a (o profilino) persone che si trovino nell'UE; prevede precise garanzie rispetto ai processi decisionali automatizzati, esigendo, almeno in ultima istanza, il filtro dell'uomo; introduce misure che mirano ad inscrivere direttamente nei sistemi e nei dispositivi le tutele per l'interessato; realizza un ragionevole equilibrio tra le esigenze di utilizzo di dati su larga scala per fini di utilità sociale con il diritto degli interessati alla protezione delle informazioni che li riguardano; riscrive il sistema sanzionatorio, adottando fra l'altro il criterio della proporzionalità della sanzione pecuniaria al fatturato.

Ebbene, mi preme evidenziare che, anche alla luce di tali importanti innovazioni, all'insediamento nel mio incarico, e nell'imminenza della scadenza del Protocollo d'intenti fra il Dipartimento e l'Autorità Garante, ho tenuto a promuovere, con la piena e convinta adesione della controparte, non un semplice rinnovo dell'atto, ma un suo vero e proprio rilancio.
Ed in effetti la nuova intesa istituzionale, sottoscritta il 6 marzo scorso, è stata revisionata nel suo contenuto, ora adeguato al GDPR - 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 per la condivisione delle notifiche di violazioni dei dati personali che ricadono nel GDPR a vantaggio del Nucleo per la Sicurezza Cibernetica. Si tratta di un significativo patrimonio di informazioni rilevanti per il Comparto. Basti considerare[10] che, solo negli ultimi sette mesi dell'anno scorso, sono giunte all'Autorità 630 notifiche di data breach, che hanno riguardato, come titolari del trattamento, soggetti pubblici (27% dei casi) e soggetti privati (73% dei casi).

[9] V. intervento dello stesso pubblicato sul sito ufficiale dell'Autorità Garante il 24 agosto 2018
[10] Secondo il Rapporto del Garante, del quale si è avuta ampia risonanza anche su fonti aperte.

In sostanza, la cooperazione tra Garante ed Organismi è stata potenziata sino a porsi come una feconda opportunità per una migliore governance digitale. A dimostrazione che quest'ultima è viabile, così come è possibile - elevando il livello della collaborazione istituzionale con sinergie concrete volte a fronteggiare i problemi posti dall'innovazione tecnologica - realizzare un bilanciamento fruttuoso fra tutela della privacy e presidio della sicurezza nazionale.

- 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 che vengano affrontate, oltre che con linee d'azione concrete, con l'abito mentale appropriato, con un elevato livello di sinergie interistituzionali, e con una profondità strategica commisurata alla portata della sfida, e fondata su una cognizione profonda delle diverse implicazioni della rivoluzione tecnologica. Nonché intervenendo, là dove 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 del 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. E 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 ad investire molto anche sul fattore umano. Sarà sempre quest'ultimo, non la tecnologia in sé che rimane solo uno strumento, a "fare la differenza": ad individuare moduli operativi, linee di intervento, proposte e soluzioni atte a farci trovare sempre "un passo oltre" agli attori e fattori ostili.
  Con due paletti ben precisi.
  Il primo paletto è che il Sistema di informazione per la sicurezza della Repubblica opera a protezione degli interessi nazionali esclusivamente nel rispetto delle leggi, e degli indirizzi, obiettivi e finalità generali deliberati dal CISR. 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, la sicurezza dell'ecosistema dell'informazione e la consapevolezza del rischio, che non possono essere percorse se non con l'ascolto attivo e con l'ingaggio responsabile di tutte le componenti del Sistema Paese. A cominciare dai soggetti obbligati della Direttiva NIS, cioè Operatori dei Servizi Digitali e

Fornitori dei Servizi Digitali, che ricordavo prima, ma senza che ci si limiti ad essi, piuttosto coinvolgendo anche il tessuto produttivo, l'Accademia, i centri di ricerca, la società civile, l'opinione pubblica.

La quinta rivoluzione ICT non richiede all'intelligence di sfigurare 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. E' questa, in estrema sintesi, la linea di pensiero che tenevo a condividere in quest'Aula.

Grazie.