CENTRO STUDI INTERNAZIONALI

IL DILEMMA DELL'INNOVAZIONE: INTELLIGENZA ARTIFICIALE E COMPARTO SICUREZZA

Di Paolo Crippa e Filippo Tansini

Dicembre 2019

CENTRO STUDI INTERNAZIONALI

Il dilemma dell'innovazione: Intelligenza Artificiale e comparto sicurezza

Si può considerare la comparsa sul mercato di tecnologie *disruptive* uno dei fattori abilitanti all'affacciarsi di nuove sfide e prove, in qualsiasi campo di applicazione. Spesso, la natura stessa di queste innovazioni supera le presenti necessità e consente di immaginare campi di applicazione fino a quel momento difficilmente ipotizzabili. In altri casi, l'avvento di nuove tecnologie rivoluziona le attività tradizionali. Ad esempio, il tumultuoso progredire delle *Information and Communications Technology* impone sempre più frequentemente la necessità di misurare la realtà con strumenti soggetti ad una rapida obsolescenza, con il rischio di ottenere risposte insufficienti o, talvolta, inadeguate. Nel caso della cosiddetta 'Intelligenza Artificiale' (IA), ci troviamo probabilmente all'intersezione tra questi due scenari. Da un lato si sta sviluppando un potentissimo strumento tecnologico di cui non è ancora possibile circoscrivere i limiti, dall'altro il contesto socio-economico è in continua trasformazione e richiede senza posa sempre nuovi strumenti per far fronte a vecchi e nuovi problemi. L'intero Sistema Paese è connesso in un'unica rete di nodi interdipendenti: dalle istituzioni, alle infrastrutture critiche fino alle aziende e al singolo cittadino. Si assiste ad una progressiva digitalizzazione e "datificazione" dei moderni enti statuali. Gli algoritmi a base IA promettono una svolta tecnologica in grado di assicurare la possibilità di quantificare, ordinare e, in ultima fase, governare l'incalcolabile e nuova mole di Big Data prodotti dalle società contemporanee. Questo è un traguardo insperato fino a pochi anni fa: una trasformazione radicale negli strumenti e nelle risorse a disposizione di amministratori e professionisti del comparto sicurezza.

Si tratta di un vero e proprio cambio di paradigma e, come tale, apre a grandi opportunità, ma potrebbe generare altrettanti rischi. E' un punto di svolta, non rinviabile, a cui occorre reagire repentinamente per non subire il ritmo incalzante del cambiamento adottando, al contempo, un approccio il più possibile robusto ed organico.

Per dare un'idea della portata di tale fenomeno, tra il 2010 e il 2018 l'Intelligenza Artificiale è stata citata in più di 1 milione e quattrocento mila pubblicazioni scientifiche, oltre 11 mila borse di ricerca, 82 mila brevetti e più di 6 mila e cinquecento documenti normativi. Il grafico in figura 1 è eloquente nel mostrare la crescita impressionante per l'interesse attorno a questo campo di studi.

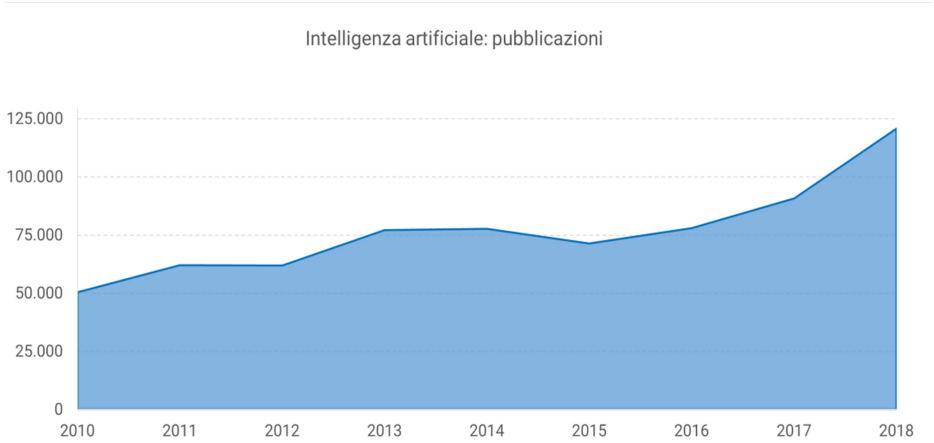

Fig.1: Andamento delle pubblicazioni scientifiche, brevetti, documenti di policy (fonte: Dimensions 2010-2018)

I dati forniti dalla piattaforma Dimensions prendono in considerazione più di cento tra le più importanti organizzazioni di ricerca scientifica di tutto il mondo. Nel solo 2018, oltre 125 mila documenti hanno discusso possibili impieghi e conseguenze dell'applicazione di algoritmi di Intelligenza Artificiale ai più disparati campi, compresi quelli più rilevanti per le competenze del comparto sicurezza.
La novità di una tecnologia come l'Intelligenza Artificiale e le incertezze legate alle promesse di miglioramento sono all'origine di un dilemma decisionale per policy maker e professionisti. In futuro sarà possibile comprendere appieno le innovazioni, i pericoli e i benefici connessi all'adozione di queste tecnologie. Tuttavia, è compito del presente confrontarsi con valutazioni e politiche di adozione. Se l'Intelligenza Artificiale può rappresentare la risposta ad alcune delle sfide poste dalla società contemporanea, l'ottimismo senza consapevolezza situazionale può condurre a scelte azzardate e implicare conseguenze impreviste. L'antinomia decisionale tra vantaggi auspicati e pericoli inattesi esige una analisi strutturata per navigare responsabilmente attraverso questa inevitabile rivoluzione tecnologica. Nei prossimi paragrafi discuteremo le principali caratteristiche dell'Intelligenza Artificiale e le sfide poste all'orizzonte del comparto sicurezza. Obiettivo dell'analisi è la proposta di un processo decisionale virtuoso, esemplificato attraverso alcuni esempi di buone pratiche e governance efficaci.

L'Intelligenza Artificiale non esiste (ancora)

La nozione condivisa di Intelligenza Artificiale (IA) presume la capacità di un sistema cibernetico in grado di affrontare problemi aperti e fornire risposte creative. Questo tipo di abilità sono tipiche di una «Intelligenza Artificiale forte», ossia di un sistema in grado di ragionare

autonomamente, imitando il modello della mente umana. Un tale processo di ricerca si propone di far emergere creatività e autoconsapevolezza in una entità tecnologica destinata a superare la specie umana (Intelligenza Artificiale generale). Questa linea di ricerca conosce un limitato sviluppo in campo scientifico contemporaneo e la c.d. «singolarità» non è una eventualità prossima all'orizzonte della storia umana.
Quanto invece è presente, con sempre maggiore frequenza, nella quotidianità di cittadini, imprese, policy-maker e comparto sicurezza è l'applicazione e la diffusione di una «Intelligenza Artificiale debole»: ossia l'applicazione di programmi progettati per risolvere specifici problemi o analisi. Algoritmi di Machine Learning (ML) e soprattutto Deep Learning (DL) hanno trovato nelle possibilità computazionali contemporanee gli elementi abilitanti per una nuova espressione di un campo di studio avviato più di 20 anni fa. Dalle reti neurali artificiali (ANN – Artificial Neural Networks) si è passati ad algoritmi di apprendimento automatico e in modo sempre più diffuso e frequente a sistemi di apprendimento neurale profondo (Fig.2).

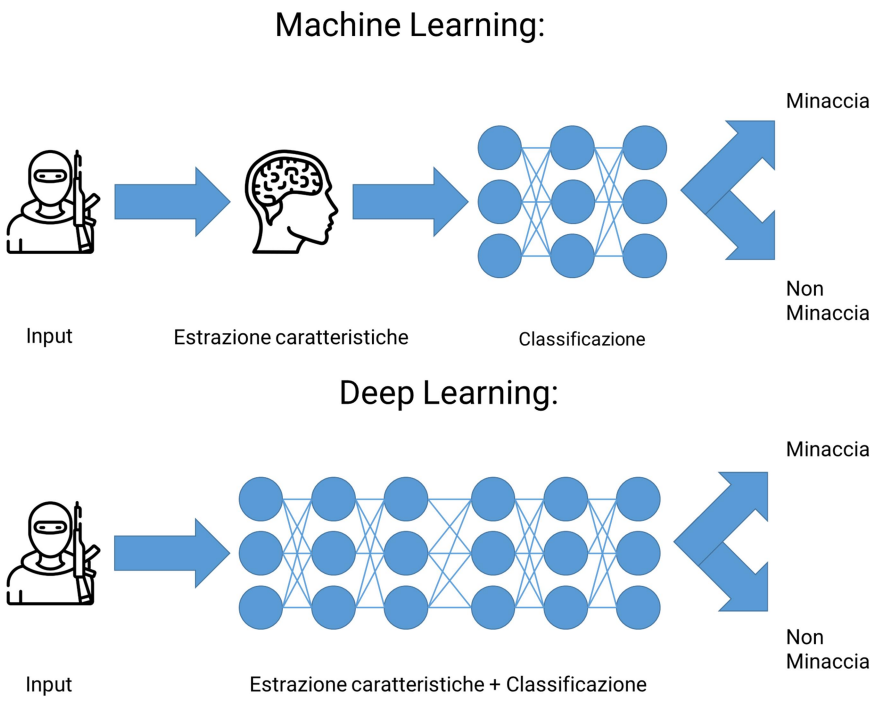

Fig.2: Schema di funzionamento degli algoritmi di Machine Learning e Deep Learning. La principale differenza consiste nell'intervento umano per l'estrazione delle caratteristiche salienti nel caso di Machine Learning. Nel caso del Deep Learning, infatti, l'apprendimento è completamente autonomo grazie a livelli sovrapposti di elaborazione.

Il cambiamento di paradigma nella ricerca scientifica e le nuove possibilità tecnologiche hanno condotto ad uno spostamento nella filosofia generale alla base di questi strumenti: non l'imitazione dei processi cognitivi umani, ma la costruzione di modelli alternativi in grado di affrontare e risolvere problemi in modo autonomo e perciò capaci di elaborare soluzioni differenti o inaspettate rispetto a quelle suggerite dai naturali processi cognitivi umani.
Machine Learning e Deep Learning, di fatto, appaiono come architetture complesse composte da unità minime di ragionamento: sistemi di classificazione, elaborazione e riconoscimento in grado di giungere a soluzioni estremamente avanzate (visione artificiale, comprensione del linguaggio naturale, *pattern recognition* etc.) pur mantenendo un circoscritto dispendio computazionale, proprio grazie all'azione sinergica e sovrapposta di numerose reti di unità minime (da cui il nome "deep learning").

Risolvere problemi (o crearne di nuovi)

A settembre 2019 è stato pubblicato sul portale di ricerca scientifica ArXive un lavoro di ricerca sostenuto dal «National Natural Science Foundation of China» e dal «National Key R&D Program of China» intitolato: «Read, Attend and Comment: A Deep Architecture for Automatic News Comment Generation» (Yang, Xu, Wu and Li, 2019). Nel paper si propone l'impiego di architetture di Deep Learning al fine di generare in modo del tutto automatizzato commenti pertinenti ad articoli di cronaca all'interno di portali di informazione online. Nel quadro di operazioni di disinformazione, tale automazione consentirebbe di perseguire obiettivi strategici (saturazione dell'orizzonte informativo, inquinamento del dibattito domestico, diffusione di *framing* favorevoli, polarizzazione del dibattito) con un'attività a basso costo e notevoli ricadute potenziali.
Reti neurali e algoritmi di Deep Learning sono attualmente applicati in numerosi ambiti del comparto sicurezza: come strumenti per l'elaborazione di modelli predittivi di crimini in ambiente urbano, al fine di ricostruire le intricate reti formate da relazioni e rapporti tra i componenti di gruppi terroristici o come chiave d'accesso ad una raccolta informativa sempre più vasta e composita (si pensi alle sfide poste dalla c.d. *all source intelligence*). Gli algoritmi svolgono già un ruolo preponderante, e in futuro entreranno in maniera ancora più pervasiva, nella gestione delle *smart city*, dei servizi essenziali (sanità, trasporti, energia, telecomunicazioni) e nella vita privata dei cittadini (es. IoT e *smart device*).

Il comparto sicurezza e Difesa si muove all'interno di un peculiare orizzonte operativo: un ambiente ad alta complessità destinato a diventare, già dall'immediato futuro, più incerto e imprevedibile. I pochi esempi citati per i più diversi settori della società civile e delle istituzioni pubbliche suggeriscono tutte le potenzialità e i rischi di applicazione dell'IA. Gli algoritmi stanno già cambiando la nostra realtà: compito di decisori e policy maker è governare questo cambiamento e saperne cogliere le opportunità inattese.

Incertezza radicale e processo decisionale

Le scoperte sono, per definizione, sconosciute e imprevedibili, gli effetti delle innovazioni non rispondono a modelli previsionali certi. Nell'universo aperto degli affari umani, l'incertezza legata alla diffusione dell'IA su scala globale suggerisce anche potenziali criticità dirompenti. La diffusione di algoritmi IA potrebbe consentire di espandere la frequenza, la forza e l'impatto di minacce già esistenti. La possibilità di automatizzare a basso *effort* attività proprie delle capacità umane, come nel caso appena discusso dei commenti alle piattaforme online, ha come conseguenza diretta anche l'aumento della platea di attori in grado di perseguire un tale attacco, con effetti di asimmetria che già caratterizzano alcune tipologie di conflitti contemporanei. L'IA è progettata per risolvere quesiti e problemi insoluti o tecnologicamente non sostenibili. Proprio per questo, l'impiego di algoritmi potrebbe creare nuove minacce e vulnerabilità inaspettate.
Infine, gli stessi processi di IA potrebbero essere oggetto di attacco: Machine Learning e Deep Learning forniscono risultati sulla base di un addestramento preventivo. Numerose ricerche recenti si sono concentrate proprio sulla possibilità di avvelenare i dati su cui si fonda questo addestramento o di manipolare i risultati finali sfruttando il c.d. effetto «black-box», cioè l'imperscrutabilità dei processi attraverso i quali gli algoritmi giungono ai risultati attesi.
Questi rischi disegnano un orizzonte decisionale costitutivamente asimmetrico, poiché una più ampia e completa conoscenza a disposizione del decisore non diminuisce l'incertezza situazionale appena descritta. Non è possibile formulare leggi generali in grado di prevedere le linee di sviluppo dell'IA e delle minacce che le applicazioni di questi algoritmi dovranno affrontare nei settori dell'intelligence, antiterrorismo, politiche pubbliche e comparto sicurezza.

Procedere con decisioni robuste verso un futuro incerto

L'ambiente contemporaneo pone sfide ad alta complessità a cui rispondere con soluzioni altrettanto complesse. L'incertezza operativa

fin qui descritta impone una area di *gap*-informativo, un dilemma tra lo stato dell'arte (sempre meno efficiente nel rispondere alle nuove minacce) e l'adozione di innovazioni dalle implicazioni sconosciute. Il processo decisionale più responsabile, secondo queste premesse, è quello in grado di individuare le soluzioni più robuste, quelle in grado di resistere al maggior numero di eventi imprevisti. La robustezza di questo processo può essere valutata attraverso la misura qualitativa di cinque descrittori decisionali: resilienza, ridondanza, flessibilità, adattabilità, completezza.

- La resilienza di una soluzione tecnologica è l'attributo del rapido recupero delle funzioni critiche. È probabile che si verifichino eventi ostili di fronte a gravi incertezze. Uno strumento è robusto contro l'incertezza se ha la capacità di riprendere rapidamente piena funzionalità e ottenere risultati rilevanti anche dopo avversità inattese.
- La ridondanza è la capacità di fornire molteplici soluzioni alternative. Questa si rivela una possibilità fondamentale nell'analisi dei teatri operativi contemporanei: sempre più frequentemente inquadrati come sistemi complessi non lineari dalle molteplici componenti e dinamiche.
- La flessibilità di una soluzione o processo decisionale è la possibilità di una modifica di strumenti e metodi in tempi rapidi, quasi in risposta diretta ai feedback rilevati.
- L'adattabilità descrive la capacità di adattare la risposta al variare delle informazioni e della consapevolezza situazionale a medio e lungo periodo. Se si considerano le caratteristiche dell'orizzonte operativo descritto, la necessità di rivalutare e rivedere valutazioni e decisioni si qualifica come caratteristica essenziale.
- Infine, la completezza delle risposte tecnologiche e di policy esprime la tensione verso una coerenza interdisciplinare a livello sistemico. Esprime la desiderabilità di un processo in grado di integrare nelle soluzioni adottate: valutazioni tecnologiche, struttura e capacità organizzative, atteggiamenti e attitudini culturali del sistema, contesto storico-sociale, possibilità economiche. Una risposta completa, talvolta in grado di tenere conto dell'intero orizzonte politico, militare, economico, sociale, infrastrutturale e informativo.

Secondo questa prospettiva, l'adozione di Machine Learning e Deep Learning risponde alla incertezza operativa contemporanea in modo particolarmente robusto quando questi sono impiegati a servizio dell'aumento delle capacità cognitive, analitiche, computazionali della mente umana, non in piena sostituzione dei processi decisionali, investigativi, analitici.

Nuovi strumenti per nuovi scenari

L'innovazione tecnologica nel campo dell'IT negli ultimi decenni ha mutato radicalmente i connotati del quadro informativo all'interno del quale si trovano ad operare gli addetti alla pubblica sicurezza. In passato, in una società non ancora digitalizzata e, per di più, divisa in blocchi ideologici difficilmente penetrabili, ci si muoveva all'interno di un mondo caratterizzato da una generale scarsità di informazioni. All'interno di tale contesto, il reperimento di informazioni era il cuore di ogni attività investigativa o di intelligence. La quantità di informazioni, infatti, non eccedeva mai in maniera significativa gli strumenti e le capacità di analisi a disposizione. Oggigiorno, al contrario, ci troviamo di fronte ad un enorme surplus di dati. Telecamere, smartphone, sistemi di posizionamento satellitare, nonché la condivisione di dati su piattaforme digitali, generano una mole di informazioni in cui è difficile districarsi. Tutto ciò, se non bastasse, è destinato a intensificarsi esponenzialmente nel prossimo futuro, con l'avvento dell'Internet of Things (IoT), che permetterà di 'sensorizzare' qualsiasi dispositivo di uso quotidiano, del 5G e dell'integrazione dei sistemi all'interno delle c.d. *smart cities*.

Di fronte a questa soverchiante marea, sembra ormai inderogabile la necessità adottare nuovi strumenti in grado di gestire tale crescente complessità. I software di Machine Learning-Deep Learning e IA oggigiorno non rappresentano soltanto una curiosa opportunità da sondare in un non precisato futuro, ma una urgente necessità per tutto il comparto sicurezza.

Attualmente la sfida non è più o, per lo meno, non più soltanto, quella di analizzare le informazioni disponibili, ma piuttosto quella di discernere le informazioni utili da quelle inutili, trovare un filo di Arianna all'interno di sconfinati labirinti numerici e semantici. Impiegare analisti secondo le classiche metodologie di ricerca informativa, sprovvisti delle recenti tecniche di big data analytics, significa sprecare enormi quantità di tempo e di risorse. Automatizzare tali processi tramite software di IA significa al contrario aumentare la produttività e destinare personale (spesso prezioso ed altamente formato) a mansioni dove l'intelligenza umana rappresenta ancora un insostituibile valore aggiunto.

La corsa tecnologica all'Intelligenza Artificiale

Nel settembre 2017, in occasione dell'inaugurazione dell'anno accademico di un'università russa, il Presidente Vladimir Putin pronunciò la seguente frase, che ottenne un'eco significativa: "Chi svilupperà la migliore Intelligenza Artificiale, diventerà il padrone del mondo". Al netto della retorica e dei toni profetici, il Presidente russo

sintetizzava un punto fondamentale: avere accesso alle più sofisticate tecnologie di IA significherà, in futuro, godere di un vantaggio competitivo esponenziale (*operational superiority*) rispetto ai propri avversari, tanto in politica estera, quanto nelle dinamiche interne agli Stati. Possedere corroborate capacità di big data analytics a supporto delle attività investigative, di intelligence e ordine pubblico, significa infatti ottenere un considerevole vantaggio rispetto a qualunque soggetto che compia atti illeciti o criminosi, il quale non disponga di sistemi altrettanto complessi che ne facilitino l'elusione. Tale disparità, inoltre, può facilmente tradursi in un utile deterrente.
Consapevoli delle opportunità che dischiude lo sviluppo di tali tecnologie, tutti i principali stati industrializzati sono impegnati da anni in una corsa tecnologica globale, che attrae sempre più capitali. Da tempo, tuttavia, appare chiaro come Cina e Stati Uniti siano saldamente alla testa di questa competizione, adottando ciascuno la propria strategia. Da un lato il governo della Repubblica Popolare Cinese agisce come vera e propria cabina di regia per lo sviluppo dell'Intelligenza Artificiale, allocando ingenti capitali pubblici e formando talenti all'interno delle proprie *state-owned tech companies*. Dall'altro l'approccio statunitense, nonché quello dei propri alleati europei, si basa sulla libera competizione tra imprese private, che dialogano con l'amministrazione statale cercando di capirne i bisogni e gareggiando per offrire le proprie soluzioni. Tale configurazione del sistema produttivo fa sì che, in tutto il mondo occidentale, i privati siano generalmente più avanti, nello sviluppo e nella implementazione di tali tecnologie, rispetto all'amministrazione pubblica. A fronte di ciò, la partnership pubblico-privato e l'outsourcing di alcuni servizi possono essere lo strumento principe per colmare tale *gap*.

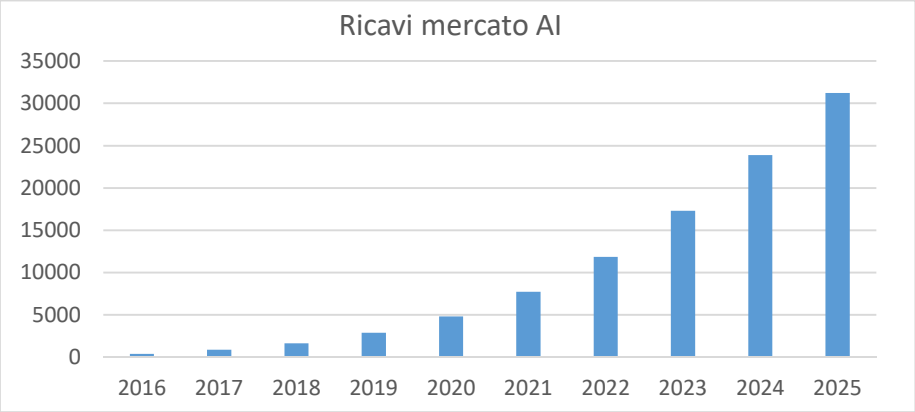

Fig.2: Proiezione che descrive l'andamento dei ricavi del mercato delle tecnologie di Intelligenza Artificiale dal 2016 al 2025. Si osserva come si tratti di un trend di crescita esponenziale (fonte: Statista 2018).

Alla ricerca di sinergie tra pubblico e privato

Non si tratta di scenari futuribili, ma di pratiche già ben rodate. In diversi Paesi, uno su tutti gli Stati Uniti, l'outsourcing di servizi di analisi di big data per il comparto sicurezza è già realtà da oltre un decennio. Nonostante si tratti di contratti generalmente protetti da forti clausole di riservatezza, è ormai noto all'opinione pubblica l'operato dell'azienda Palantir Technology a supporto delle attività di polizia, FBI, ICE, CIA, Pentagono, NSA e di un variegato novero di agenzie di *law enforcement*. Palantir, che ad oggi è una delle principali *tech companies* americane, fornisce fondamentalmente software in grado di raccogliere e analizzare grandi quantità di dati, provenienti da diverse tipologie di fonti, per metterli in relazione e ricostruire legami. Palantir non si limita soltanto a fornire accesso alle proprie piattaforme (per lo più *user-friendly*, che possono essere utilizzate agevolmente anche da un semplice agente di polizia), ma disloca i propri ingegneri all'interno degli uffici federali per svolgere i compiti più complessi o per supervisionare e coordinare le attività di analisi. Questo strumento, che vanta oltre dieci anni di fruttuoso impiego, dal supporto delle attività CIA in Afghanistan alla gestione dell'immigrazione, sembra rispondere in buona misura agli indicatori di robustezza elencati in precedenza. Si tratta di una tecnologia in grado di aggregare dati provenienti da più fonti diverse, siano esse immagini satellitari, dati anagrafici, profili social, account bancari o segnali GPS (completezza). Può essere impiegata per espletare diversi compiti e all'interno di diversi settori, dal *counter-insurgency* alla *business intelligence* (flessibilità e adattabilità). L'uomo ovviamente non è escluso, ma rimane anzi il cardine dell'intero processo analitico, chiamato da ultimo a scegliere tra le diverse soluzioni proposte (ridondanza).

Per governare la complessità

Quello appena descritto è soltanto un esempio di come gli strumenti di big-data analytics basati su algoritmi IA possono portare un valore aggiunto e migliori risultati alle attività del comparto sicurezza. In Italia, così come in Europa, per quanto strutturalmente in ritardo nella corsa all'Intelligenza Artificiale rispetto ai due giganti, disponiamo di network di vere eccellenze tecnologiche, che, se non per dimensioni, possono competere qualitativamente con i noti *big player*. Essendo lo Stato *de facto* monopolista dei servizi di pubblica sicurezza, dunque principale investitore di risorse nel settore, ci si attende assuma un ruolo sempre più proattivo nello stimolare la ricerca tecnologica, nello sperimentare e nell'implementare nuovi sistemi.

In futuro, infatti, sarebbe auspicabile maggiore agilità e minore farraginosità burocratica nei rapporti tra amministrazione pubblica ed imprese, dal momento che il ritmo dell'innovazione tecnologica, in molti casi, supera di gran lunga la velocità di adattamento dell'apparato statale. Certamente l'amministrazione pubblica non dovrebbe abbandonarsi incautamente ad un cieco entusiasmo tecnologico, alla luce dei potenziali rischi che esso comporta. Al contrario, sarebbe auspicabile mantenesse uno scrupoloso ruolo di supervisore, forte di strumenti di giudizio e governance corroborati dalle buone pratiche a livello internazionali e valutati, ad esempio, attraverso gli indicatori di robustezza citati in precedenza. Al contempo, due elementi emergono come urgente necessità per la pubblica amministrazione: una esaustiva conoscenza situazionale delle più recenti istanze tecnologiche e un' approfondita analisi delle soluzioni possibili per colmare eventuali *gap* capacitivi, vagliando anche ipotesi innovative e strade non ancora battute. Compiere tale processo significherebbe non soltanto dischiudere opportunità di sviluppo per l'intero Sistema Paese, ma lavorare alla costruzione di uno Stato più efficiente, in grado di navigare consapevolmente nel *mare magnum* dei big data, senza esserne travolto.