



# Intelligence e IA

Il binomio perfetto?

ANTONIO TETI

*Il mondo dell'intelligence, da sempre votato alla raccolta e all'analisi d'informazioni sensibili per garantire la sicurezza nazionale e contrastare minacce interne ed esterne, si trova oggi a operare in un contesto radicalmente mutato. L'intelligenza artificiale (IA), con le sue capacità di apprendimento automatico, analisi predittiva e gestione di enormi quantità di dati, è diventata una risorsa imprescindibile per le Agenzie di tutto il mondo. L'avvento dell'IA nell'intelligence può consentire di produrre vantaggi significativi: velocità senza precedenti nell'elaborazione di dati, capacità d'individuare pattern nascosti tra informazioni apparentemente scollegate e una maggiore automazione di operazioni complesse.*

**ANTONIO TETI** Responsabile del settore Sistemi informativi e innovazione tecnologica dell'Università G. D'Annunzio di Chieti-Pescara, dove ricopre anche incarichi di docenza. È esperto di Ict governance, cybersecurity e cyberintelligence e autore di numerosi libri e pubblicazioni scientifiche.

---

**L'**evoluzione dei social media ha prodotto, quasi imprevedibilmente, la nascita e lo sviluppo delle *online relationships*, ovvero relazioni virtuali in cui la ricerca della vicinanza, l'intimità e il sostegno emotivo, peculiarità che governano l'esistenza dell'individuo, il quale le conserva e alimenta durante tutta la propria vita, possono esprimersi in maniera diversa dal mondo reale, sfruttando tutte le potenzialità offerte dall'ecosistema digitale in cui siamo immersi. La stessa identità personale è fortemente condizionata dal rapporto con gli altri e, pertanto, risulta anch'essa influenzata dalla digitalizzazione delle relazioni umane. Questa germoglia e si estende sulla base delle attuali e crescenti difficoltà che si riscontrano nell'attivazione d'interazioni dirette nella realtà, in cui si mescolano bisogni, ansie, desideri e timori in un mix di ritmi frenetici quotidiani. Gli eventi che caratterizzano questo particolare momento storico a livello planetario stanno producendo conseguenze sull'individuo e sulla sua condizione, inducendolo sempre più a ricercare nel virtuale ciò che il reale non può consentire: connettersi con chiunque eliminando qualsiasi tipo di barriera fisica e temporale, gestire gli scambi secondo la propria disponibilità del momento ed evitare tutti i possibili conflitti o le incomprensioni che possono scaturire nelle frequentazioni quotidiane.

Il rapporto virtuale porta con sé una sottostante paura della relazione reale, che può essere alimentata da una carenza di stima di sé stessi, dalle convinzioni di non essere interessante per gli altri, di non riuscire in alcun modo a soddisfare i propri desideri o di risultare incapace su piani diversi, da quello lavorativo / professionale a quello affettivo. In un legame online si può usufruire del distacco reale tra le parti nonché dell'anonimato. Si possono generare pulsioni sul proprio interlocutore e gestirle grazie alla pubblicazione di post, immagini, video, reazioni e commenti. Di conseguenza, le relazioni online offrono molteplici vantaggi per quanto concerne l'attivazione di rapporti personali.

Gli studi in materia hanno condotto alla definizione di nuovi percorsi di ricerca nell'ambito delle neuroscienze sociali, anche tenendo conto delle diversità esistenti, di seguito evidenziate, tra le relazioni sociali che si sviluppano nel mondo reale e quelle virtuali.

*Riduzione / azzeramento delle regole sociali.* Nel mondo virtuale le norme comportamentali che regolano le interazioni *face-to-face* tra due individui vengono spesso a mancare. Ad esempio, l'attribuzione di significati alla gestualità, alle espressioni visive, al tono della voce e alla cura dell'immagine è un elemento cognitivo che risulta completamente assente, contrariamente a quanto accade in una reciprocità personale nel mondo reale. Allo stesso modo, online è persino osservabile una sostanziale violazione delle norme di educazione.

*Azzeramento delle barriere geografiche e temporali.* I social media offrono la possibilità di entrare in contatto con soggetti ubicati in qualsiasi Paese del Pianeta. Le tempistiche dedicate alle interazioni sociali online possono variare unicamente in funzione della disponibilità degli utenti, senza altri limiti di sorta.

*Azzeramento della risposta immediata.* Le conversazioni tra gli utenti gestite attraverso applicazioni instant messaging come WhatsApp, Telegram, Signal, Facebook Messenger, Instagram, oppure mediante la pubblicazione di post sui diversi social media sono caratterizzate da una peculiarità: la gestione delle pause. Se in un'interazione tradizionale i tempi di attesa per una risposta richiesta a fronte di una domanda sono ridottissimi, in un'interlocuzione online si è disposti ad accettare pause



che possono variare notevolmente, senza che tali ritardi producano reazioni di tipo diverso da parte degli interlocutori. Va altresì evidenziato che le conversazioni basate su contenuti scritti nei post o attraverso le applicazioni di messaggistica, a differenza di una conversazione a voce, permangono nel tempo.

*Anonimato.* Una delle maggiori tipicità dei social media risiede nell'opportunità di creare profili in cui la propria identità può essere alterata o resa completamente non visibile, contrariamente a quanto accade nelle relazioni nel mondo reale. Ciò permette di costruire account sulla base degli obiettivi perseguiti e finanche la realizzazione di profili completamente falsi (*fake profiles*).

*Gestione dei contenuti.* Diversi studi e ricerche hanno confermato una naturale propensione degli utenti a rivelare aspetti e informazioni private all'interno dei social media, contrariamente a quanto accade nei rapporti diretti nel mondo reale. Anche la strutturazione dei contenuti può fornire un significativo contributo per la comprensione delle caratteristiche del profilo (lunghezza del messaggio, presenza d'immagini, video, emoticons ecc.).

In virtù dello scenario descritto, appare evidente come sia realizzabile, nel mondo virtuale, la progettazione e la gestione di attività finalizzate all'analisi e alla comprensione dei tratti psicologici. È quindi importante per l'intelligence conoscere e valorizzare tutti gli aspetti del fenomeno a scopo difensivo, soprattutto in considerazione dell'uso diffuso in ambito commerciale e da parte di attori informatici esteri molto orientati a operare nell'ecosistema digitale secondo modalità aggressive.

Il termine *cyber profiling* si riferisce esattamente a quell'insieme di tecniche e pratiche utilizzate per raccogliere e analizzare dati provenienti da ambienti digitali al fine d'identificare, capire e, in alcuni casi, prevedere e modificare i comportamenti online. Nato inizialmente in ambiti come la cybersecurity e le indagini digitali, il *cyber profiling* ha oggi applicazioni che spaziano dalla sicurezza nazionale al marketing, fino alla gestione della reputazione aziendale. Con l'aumento esponenziale delle attività online, è diventato uno strumento fondamentale per comprendere le persone e le loro intenzioni nel mondo digitale.

Il *profiling* digitale si fonda su un'accurata raccolta e successiva interpretazione di diversi tipi di dati, spesso ottenuti in tempo reale e in grandi volumi. La maggior parte di essi si divide in due categorie principali: i dati espliciti, come i post sui social media o le informazioni che un utente inserisce in un form, e quelli impliciti, come i metadati associati alle sue attività (ad esempio l'orario di connessione o la posizione approssimativa).

Le principali fonti di dati utilizzate nel *cyber profiling* includono:

- *social media*. Piattaforme come Facebook, Twitter e Instagram sono una miniera d'informazioni personali. I post, i commenti e i "like" rivelano preferenze, legami sociali e interessi personali;
- *motori di ricerca e siti web*. Le ricerche eseguite su Google, Bing o altri motori di ricerca offrono indizi sulle intenzioni e sugli interessi dei soggetti;
- *e-commerce e transazioni online*. Gli acquisti, le recensioni e le preferenze di prodotto raccontano molto sullo status socio-economico e sui gusti personali;
- *registri di rete*. I dati tecnici, come gli indirizzi IP e gli orari di connessione, permettono d'identificare modelli di comportamento e tracciare connessioni geografiche.

Il *cyber profiling* si basa prioritariamente su ricerca, raccolta e analisi dei dati provenienti dal mondo virtuale (email, social media, forum, darknet) per cercare di costruire un profilo del soggetto analizzato o di un gruppo di utenti. I dati più rilevanti estraibili dalle attività di analisi devono includere, innanzitutto, le caratteristiche: *personali* (età, genere, nazionalità, livello culturale); *psicologiche* (tratti di personalità, motivazioni, disturbi comportamentali); *comportamentali* (schemi d'uso, frequenza di attività, abitudini linguistiche).

Successivamente alla fase di raccolta, si procede con l'estrazione e il filtraggio mediante l'adozione di tecniche e strumenti come l'*analisi comportamentale e linguistica*, il *machine learning* e il *deep learning*. La prima focalizza l'attenzione sull'utilizzo di tecniche psicologiche e linguistiche per tentare di comprendere lo schema psicologico degli utenti. È utilizzata specialmente nei settori del cybercrime, del cyberbullying e di altre forme di devianza digitale. È importantissima soprattutto per le Forze dell'ordine

e per gli *intelligence analysts* al fine di definire i lineamenti psicologici e comportamentali dei profili anonimi o degli utenti che si nascondono dietro pseudonimi o *fake profiles*. Assume, inoltre, un ruolo fondamentale per la conduzione di attività finalizzate al contrasto alle moderne minacce digitali, ma richiede un costante aggiornamento e il coinvolgimento di professionalità variegate. In tal senso, anche rispetto al *cyber profiling*, è da considerarsi una materia interdisciplinare, in cui si miscelano settori scientifici come la psicologia, la linguistica, l'informatica e la criminologia. In funzione dell'inesauribile mole di dati fruibili online, inoltre, l'utilizzo di piattaforme d'intelligenza artificiale (IA) rappresenta una scelta imprescindibile. Gli algoritmi di apprendimento automatico consentono di analizzare rapidamente enormi quantità di dati, identificando quegli schemi complessi che sarebbero impossibili da rilevare manualmente. L'utilizzo di piattaforme d'IA per le attività di *cyber profiling* stanno producendo una rivoluzione metodologica sul piano della conduzione di attività di ricerca, individuazione e prevenzione delle minacce digitali, come il cyber terrorismo e lo spionaggio cibernetico. Attraverso l'analisi automatizzata di enormi quantità di dati, le piattaforme d'IA sono in grado di identificare rapidamente i pattern comportamentali e linguistici utili per tracciare dei profili sospetti, rilevare delle anomalie presenti nei social media e, di conseguenza, anticipare eventuali rischi derivanti dalla veicolazione di contenuti potenzialmente pericolosi.

In sintesi, l'utilizzo dell'IA nel mondo dell'intelligence può consentire:

- *il riconoscimento avanzato di modelli e l'analisi predittiva*. Gli algoritmi di apprendimento automatico sono in grado di analizzare vasti set di dati relativi al comportamento dell'utente, come i contenuti generati nelle relazioni virtuali, le immagini e i video pubblicati, le tipologie di emoticon utilizzate, il sentiment sui contenuti visualizzati e l'engagement generato dai messaggi. Ciò permette la rapida identificazione di modelli "d'interesse" che potrebbero essere difficili da rilevare per gli analisti umani. Questa capacità autorizza le Agenzie d'intelligence ad allocare le proprie risorse umane in modo più efficace, concentrando gli sforzi sul *lead* e sulle fonti di maggiore interesse. Ad esempio, i sistemi d'IA possono elaborare e analizzare rapidamente lo storico di dati presenti sul web e



sui social media, identificando quei modelli di comunicazione e quelle tendenze comportamentali che possono rivelarsi particolarmente efficaci nell'interazione con utenti appartenenti a diverse comunità virtuali. Un'attività, quest'ultima, che può supportare la previsione di eventi futuri con un grado di accuratezza che sarebbe impossibile per gli *intelligence analysts*. Questa facoltà predittiva può essere inestimabile nell'affrontare in modo proattivo potenziali minacce alla sicurezza o nell'identificare nuove opportunità di raccolta informativa a fini difensivi e/o preventivi;

- *l'elaborazione linguistica in tempo reale e l'analisi del contesto culturale*. L'elaborazione avanzata del linguaggio naturale (*natural language processing*) sta perfezionando la traduzione in tempo reale e l'analisi del contesto culturale. Ciò favorisce una crescita qualitativa dell'analisi intelligence poiché è in grado d'incrementare la sicurezza e l'efficacia delle attività condotte dagli operatori sul campo. Gli strumenti basati sull'IA possono aiutare gli agenti a muoversi in ambienti linguistici e culturali non familiari, fornendo feedback e *indicazioni-guida* immediati in scenari sociali ed etnici particolarmente complessi. Questo elemento può coadiuvare notevolmente l'abilità dell'agente di produrre rapidamente un report qualitativamente superiore, grazie alla possibilità di raccogliere informazioni più accurate, evitando di commettere errori d'interpretazione e valutazione delle fonti e delle situazioni analizzate;
- *la riduzione del carico cognitivo e il miglioramento del processo decisionale*. I sistemi d'IA artificiale stanno anche contribuendo alla riduzione del carico cognitivo degli operatori d'intelligence, assistendoli nella raccolta dati e nella fase di *raffinazione*. Simile esito può consentire agli operatori Humint di concentrarsi maggiormente sulla strategia di alto livello e sul processo decisionale critico. Nella gestione di alcune attività di routine, l'IA può riorientare le mansioni degli *intelligence analysts* verso attività che richiedono competenze unicamente umane, come intuizione, empatia e ragionamento complesso;
- *il miglioramento della convalida della fonte e della verifica delle informazioni*. Uno degli aspetti più impegnativi della Humint è la verifica dell'affidabilità delle fonti e dell'accuratezza delle informazioni. L'IA può svolgere un ruolo cruciale in questo processo, incrociando le informazioni

prelevate da un numero ampio di database interrogati, identificandone le incongruenze e fornendo una valutazione più oggettiva. Gli algoritmi di apprendimento automatico possono analizzare i pattern riferibili alle informazioni precedentemente comunicate da una fonte, confrontandole con i nuovi modelli di comunicazione utilizzati dalle fonti e dalla descrizione degli eventi cui si riferisce l'attività di raccolta informativa. Sarà così possibile rilevare facilmente sottili indicatori d'inganno nelle comunicazioni scritte o verbali.

---

### **Intelligence and AI. Is it the Perfect Match?**

The world of intelligence has always dealt with the collection and analysis of confidential information to ensure national security and counter domestic and foreign threats. But intelligence today operates in a radically new context. Artificial intelligence (AI) is equipped with tools for machine learning, predictive analysis and management of enormous amounts of data. For this reason, AI has become an indispensable resource for agencies all around the world. The advent of AI in intelligence paves the way to significant opportunities: unprecedented speed in data processing, the ability to identify hidden patterns in seemingly unrelated information and greater automation of complex operations.

---

**Didascalie e crediti**

**A p. 145:** (Wirestock Creators / Shutterstock). **A p. 148:** (Wirestock Creators / Shutterstock). **A p. 152:** (Wirestock Creators / Shutterstock).