# Intelligenza Artificiale e Machine Learning - Intervista ad Andrea Zapparoli Manzoni

**Date :** 2 febbraio 2018

Intervista ad **Andrea Zapparoli Manzoni**, esperto di cyber security

**Per quanto l'espressione 'intelligenza artificiale' sia ormai di uso comune, si tratta di una tecnologia relativamente giovane: se già nel 1943 i ricercatori Warren McCulloch e Walter Pitts propongono un modello di neurone artificiale, solo a partire dagli ultimi due decenni si sono avute esperienze significative nella sua applicazione. Qual è oggi lo stato di avanzamento e cosa possiamo aspettarci dal prossimo futuro?**

Esistono tre filoni di applicazione dell'intelligenza artificiale, tutti interessanti: il primo è quello degli oggetti, individualmente "stupidi" ma che una volta dotati di microprocessori, anche non troppo potenti, saranno in grado di cooperare tra di loro come uno sciame (al riguardo parliamo infatti di *swarm intelligence*) per ottimizzare le prestazioni, fare autodiagnosi dei problemi e molto altro. Questi oggetti, collocati in una dimensione intermedia fisico-digitale che definiamo *phygital,* diventano pericolosi solo se compromessi in grande numero; è già avvenuto con le botnet scritte per attaccare apparati dell'IoT (a cominciare da Mirai proseguendo con i suoi successori, come Nirvana).

Ci sono poi quelli che una volta chiamavano "sistemi esperti" e che oggi definiamo *machine learning*. Qui si presenta un problema rilevante: i loro input, molto difficili da proteggere, possono essere "avvelenati" dall'esterno secondo uno schema di *garbage in/garbage out* che apre a ricadute potenzialmente gigantesche (pensiamo ad esempio al loro utilizzo nel settore creditizio). Il *poisoning* dei sistemi altrui rappresenterà anche il nuovo confine del *cyberwarfare*: non si tratta di fantascienza ma di un futuro quanto mai vicino.

**Nel 2014 il Ceo di Tesla Elon Musk, dopo aver letto in anteprima il libro *'Superintelligence'* del docente di Oxford Nick Bostrom, affermò in un tweet che iniziava a ritenere l'intelligenza artificiale "più pericolosa del nucleare". Concorda con una visione così pessimistica?**

Qui arriviamo al terzo filone. La superintelligenza è una questione filosofica: cosa accadrebbe nel momento in cui sul nostro pianeta esistessero esseri intelligenti come - o più di - noi? È

facile immaginarne gli utilizzi in campo militare, ad esempio un'evoluzione degli attuali droni che gli consenta di operare autonomamente la valutazione costi/benefici prima di procedere a un attacco, di fatto sostituendosi a qualunque giudice o giuria. I risvolti etici sono inimmaginabili e la mia sensazione è che si tratterà di un cambiamento straordinario, non solo sul piano pratico ma nel nostro stesso modo di percepire il mondo che ci circonda.

Se non sono pessimista è perché non credo arriveremo a questo: i costi sono così alti e la strada da percorrere talmente accidentata, che probabilmente ci si fermerà prima che queste tecnologie abbiano modo di esprimere tutta la loro pericolosità.

**I social network stanno cambiando il nostro mondo. Tutti sono connessi. Non sempre però l'utente medio è consapevole dei rischi legati alle nuove tecnologie. C'è il grande problema della privacy anche perché gli Stati nazionali non sembrano avere la forza di intervenire. Secondo lei, si può fare qualcosa per cambiare questa tendenza?**

Oggi siamo parte di un'umanità connessa, sempre più dipendente dal riflesso biochimico che alimenta la follia collettiva dei social media (è dimostrato come ricevere *like* attivi i recettori della dopamina, legati al piacere e alla gratificazione) conferendo a queste tecnologie un'aura di esperimento antropologico e genetico. La privacy è morta perché questo settore prospera nella mancanza di regole, tanto fiscali quanto di comportamento. Ricordate ciò che avvenne con la Standard Oil di Rockfeller all'inizio del '900? Si trattava delle società monopolista del petrolio sul mercato statunitense, alla quale il governo impose in chiave antitrust la scissione da cui nacquero le cosiddette Sette Sorelle. Questo tipo di intervento oggi non sembra immaginabile perché gli Stati nazionali non hanno la medesima forza normativa nei confronti delle *corporations* e delle loro attività di lobbying; d'altro canto nel mercato attuale eventuali normative a livello nazionale risulterebbero inapplicabili, occorrendo uno sforzo globale difficilmente ipotizzabile.

Un po' come per i fumatori, la consapevolezza dei rischi non è sufficiente a generare la volontà di sottrarsi al meccanismo - sottrazione che comunque, nel caso della connessione, sarebbe ormai concretamente impossibile. Sia per questo stato di dipendenza sia perché le minacce migrano da un canale all'altro evolvendosi più velocemente degli strumenti pensati per contrastarli (ad esempio rispetto a qualche anno fa oggi ci arriva molto meno spam via mail, ma è migrato su Facebook e Whatsapp dove è più difficile controllarlo) il lavoro di prevenzione risulta difficilissmo. C'è anche la trappola dell'economicità: un canale social effettivamente tutelato non potrebbe essere *free*, perché imporrebbe elevatissimi costi di gestione. Dato che finora non si è saputo - o voluto - sviluppare tecnologia comunicativa affidabile, è difficile pensare di mettere in sicurezza un sistema che non è nato con le giuste caratteristiche.

**I campi di applicazione della AI vanno - solo per fare qualche esempio - dall'analisi finanziaria all'automazione industriale, dalla diagnostica medica alla traduzione linguistica, lasciando così immaginare l'enorme pervasività di questa tecnologia sia nelle attività di governi e imprese, sia nella vita quotidiana delle persone e - di conseguenza - la sua attrattività per chi lucra sulle falle della sicurezza informatica. Stando così le cose, dove ritiene si annidino le maggiori vulnerabilità?**

Il principale problema è di natura economica: ad oggi nessuno ha ancora messo in campo le enormi risorse necessarie a cambiare davvero l’approccio in tema di sicurezza, e la conseguenza è che mancano sia obblighi per i produttori sia consapevolezza tra gli utenti finali. Se le automobili di oggi costano circa il doppio rispetto a trent’anni fa è perché nel frattempo sono intervenuti grossi investimenti sul piano dei dispositivi di sicurezza; oggi nessuno si sognerebbe di chiedere una macchina che fosse priva di ABS o airbag, anche perché non verrebbe risarcito dall’assicurazione in caso di incidente. Così si è creato un mercato di automobili sicure. Nell’informatica questo non è ancora avvenuto e, in assenza di vincoli, la sicurezza continua a essere percepita come un costo superfluo. Per me ad esempio creare uno strumento come Whatsapp (adottato nel giro di pochi anni da due miliardi di persone) senza prevedere aspetti di security, è criminale - ma non esistono obblighi normativi in questo senso e anche se esistessero, come dicevamo, sarebbero di ardua applicazione.

Non credo ci siano formule magiche, si potrebbero sperimentare molti modi (assicurazioni obbligatorie per gli utenti e multe salatissime per i produttori irresponsabili, volendo immaginarne alcune) ma direi senz'altro che la maggiore vulnerabilità risiede in questo approccio: i produttori restano indenni da responsabilità anche in caso di danni rilevantissimi, per cui non sono spinti a investire sul piano della sicurezza allo scopo di prevenirli. Cambiare questo paradigma è difficilissimo ma, se vogliamo invertire la rotta, credo sia l’unica strada da percorrere.

A cura della Redazione