

MACHINE LEARNING: BREVE INTRODUZIONE E ASPETTI CRITICI

Il *machine learning* rappresenta una delle innovazioni tecnologiche più rilevanti degli ultimi tempi, ma quali sono rischi per nostri dati e privacy? Quali i vantaggi e quali gli svantaggi?

AUTORI: Aurora Agostini e Jessica Giussani

SOMMARIO

MACHINE LEARNING.....	2
Cos'è il Machine Learning? Come funziona?	2
Diversi tipi di machine learning.....	2
L'importanza del machine learning.....	3
Una tecnologia alla portata di tutti e per tutti i giorni.....	3
AI come booster per l'istituzione pubblica	4
AI: un puzzle delicato	4

MACHINE LEARNING

Cos'è il Machine Learning? Come funziona?

Il termine *Machine Learning* si riferisce ad una sottocategoria dell'intelligenza artificiale che consente alle macchine di AI di migliorare le loro capacità e prestazioni nel tempo. Il metodo di funzionamento di una *machine learning* utilizza **algoritmi** per sviluppare un **modello di ragionamento** basato su un set di dati predisposto e per poi aggiustarlo nel tempo sulla base dell'esperienza. In altre parole, questi algoritmi sono in grado di adattare la loro struttura ed il loro funzionamento sulle basi dei problemi che risolvono – più algoritmi vengono risolti, più le macchine imparano a correggere e migliorare il sistema. Queste peculiarità fanno sì che gli algoritmi vengano utilizzati per creare modelli di machine learning sempre più precisi ed accurati, facendo in modo che acquisiscano una certa "**autonomia**" nel processo.

Il punto di partenza di ogni *machine learning* è un insieme di dati, forniti dallo sviluppatore, composti da **situazioni** e **soluzioni variabili**, le quali rispettivamente rappresentano esempi concreti delle varie problematiche che il sistema può trovarsi a dover affrontare e le possibili soluzioni.

La prima persona a mostrare interesse in questo settore fu **Alan Turing**, il quale negli anni '50 del novecento sottopose all'interesse pubblico la necessità di algoritmi capaci di analizzare i primi prototipi di *machines learning*. Da allora questa tecnologia ha continuato a migliorare e ad oggi ci permette di fare cose incredibili.

Diversi tipi di machine learning

Sulla base di come i sistemi raccolgono informazioni ed imparano da esse, è possibile identificare tre tipologie di strutture di machine learning:

- ***Supervised machine learning***: in questo caso vengono forniti al computer i dati relativi all'input, ovvero i problemi che verranno presentati ad esso, e le informazioni sugli obiettivi desiderati, ovvero la soluzione dei problemi. Il sistema ha l'obiettivo di identificare una regola generale che connette i dati in ingresso ai dati in uscita, in modo che possa poi riutilizzare questa regola per compiti simili. In sintesi, vengono forniti esempi di input e output affinché il sistema apprenda la relazione tra di essi e la applichi a nuovi casi.
- ***Unsupervised machine learning***: i sistemi di apprendimento automatico appartenenti a questa categoria sono forniti di un insieme di dati costituito solo da dati di input, senza alcuna indicazione dell'output desiderato. Lo scopo di questo tipo di sistemi è quello di "scoprire" schemi e modelli nascosti, ovvero identificare una struttura logica nei dati di input senza che questi siano stati precedentemente etichettati.
- ***Reinforcement learning***: in questo caso il sistema migliora il suo modello di apprendimento analizzando non solo le esperienze passate, ma anche l'ambiente circostante. La particolarità del metodo di apprendimento per rinforzo risiede nel meccanismo di **ricompensa/punizione** che regola il funzionamento del sistema. Infatti, interagendo con i dati in input, provenienti sia dal dataset che dall'ambiente, il sistema viene premiato per il raggiungimento di alcuni obiettivi definiti e punito per comportamenti indesiderati.

È importante menzionare anche il *deep learning*, una sottocategoria del *machine learning* molto simile al *reinforcement learning*. Il ***deep learning*** crea in modo autonomo il proprio modello di ragionamento da un insieme di dati. Tuttavia, a differenza del *reinforcement learning*, non procede per tentativi ed errori. In particolare, il deep learning applica le regole di ragionamento estratte da "vecchi" dataset a quelli nuovi al

fine di identificare le caratteristiche rilevanti. Per questo motivo, il deep learning è principalmente utilizzato per attività riconoscimento come quello vocale o di immagini.

L'importanza del machine learning

Indipendentemente dalla distinzione tra i tipi di sistemi di apprendimento, i dati utilizzati nella **fase di addestramento** (set di dati) svolgono un ruolo fondamentale nel funzionamento del sistema, poiché l'algoritmo ha bisogno di una grande quantità di informazioni a sua disposizione per sviluppare un modello di ragionamento in grado di risolvere problemi in modo preciso ed efficace. I risultati che possono essere ottenuti con il machine learning non possono essere raggiunti dalla mente umana, che non può elaborare una quantità così grande di informazioni. È quindi chiaro che questo strumento ha un enorme potenziale.

Basti pensare a come il machine learning abbia cambiato il sistema finanziario con la previsione dei dati e il trading nel **mercato delle criptovalute**: al momento ci sono più di 20mila criptovalute diverse e l'IA è in grado di fornirci previsioni e grafici per ognuna di esse in ogni momento della loro esistenza nel metaverso. Questo sarebbe certamente impossibile per la mente umana.

Una tecnologia alla portata di tutti e per tutti i giorni

È spesso pensato che questo strumento abbia applicazioni solo in campi molto tecnici, come la scienza, la medicina, l'ingegneria spaziale o altre branche non comunemente comprese dai non-tecnici. Questo è un errore molto comune, poiché il machine learning ha molte applicazioni nella vita quotidiana; anche se, naturalmente, implica l'uso della tecnologia. Un'applicazione classica del machine learning è nel settore dell'**automazione domestica**: gli strumenti che utilizzano il riconoscimento vocale per imparare nuove parole o modi di parlare seguendo i comandi vocali che vengono dati loro sono molto diffusi.

Pertanto è possibile dire che, per la prima volta nella storia umana, esistono strumenti capaci di tracciare ciò che milioni di persone fanno ogni giorno: fino a non molto tempo fa, solo le persone di alto rango sociale potevano vantare biografi che registravano le loro abitudini, interessi e comportamenti, ma oggi siamo tutti sotto i riflettori (anche se spesso involontariamente). Infatti, uno dei più comuni utilizzi del machine learning è la **profilazione** degli individui al fine di consentire alle aziende di creare annunci mirati. Ciò significa che è possibile proporre pubblicità strettamente legate agli interessi di ciascun utente, poiché le sue esigenze e preferenze sono riconosciute grazie all'analisi della sua "**impronta digitale**", ovvero il *cluster* di dati generati dall'utente durante l'utilizzo di app e la navigazione su internet.

Un esempio di come questa attività di profilazione incida sulla vita delle persone può essere ad esempio l'uso di dispositivi indossabili come gli **smartwatch**, che attraverso l'analisi dei dati raccolti, come i passi effettuati durante il giorno e la traccia del battito cardiaco, è in grado di identificare e tenere traccia delle varie attività che l'individuo che lo indossa svolge durante il giorno. Ad esempio, monitorando la variabilità tra i battiti, lo smartwatch può indicare quando un individuo è stressato, poiché una diminuzione della variabilità indica livelli di stress più elevati, mentre un aumento indica livelli di stress più bassi. Un'altra cosa tracciabile è l'attività fisica, poiché qui lo smartwatch può misurare quando il nostro battito cardiaco si accelera e quando rallenta durante il sonno, oltre a molte altre condizioni che è possibile monitorare. Un ulteriore mezzo per profilare gli individui sono le auto e altri mezzi di trasporto condivisi, che, tracciando i nostri spostamenti attraverso la geolocalizzazione, sono in grado di conoscere i luoghi che gli individui frequentano e, di conseguenza, conoscere i loro interessi.

AI come booster per l'istituzione pubblica

Vale la pena sottolineare che l'intelligenza artificiale non attira l'attenzione solo delle aziende private. Infatti, il settore pubblico ha recentemente mostrato un certo interesse verso l'uso dei sistemi AI. Alcuni studiosi si riferiscono a questa "nuova era" come "**era dello Stato Digitale**", sottolineando la trasformazione radicale delle attività pubbliche attraverso l'introduzione di nuove tecnologie. Ad esempio, il Piano Coordinato dell'Unione Europea sull'Intelligenza Artificiale ha come obiettivo l'uso delle tecnologie dell'informazione e delle nuove tecnologie per **innovare anche l'Amministrazione Pubblica**. Seguendo le iniziative adottate da altri paesi europei, l'Italia ha avviato un processo di de-burocratizzazione e semplificazione delle procedure, che porterà alla creazione di una struttura Big Data centralizzata unica, al fine di evitare la duplicazione o la significativa perdita di informazioni e sfruttare la grande quantità di informazioni disponibili per l'Amministrazione Pubblica.

Se ne deduce che la tecnologia avrà un impatto su diverse aree, dai servizi pubblici all'amministrazione della giustizia. Per quanto riguarda l'amministrazione della giustizia, un'applicazione particolarmente interessante del machine learning è l'uso dei cosiddetti **sistemi di decisione automatizzati**, ovvero sistemi di intelligenza artificiale che sostituiscono il giudice nella decisione di un caso. L'Estonia è un pioniere in questo campo, poiché nel 2019 ha introdotto la piattaforma "X-road" per la risoluzione di piccole controversie con un valore inferiore a 7.000,00 EUR.

AI: un puzzle delicato

Anche se rappresenta un'opportunità interessante per le aziende e le istituzioni pubbliche, è fondamentale non dimenticare che il machine learning comporta anche seri **rischi**, in particolare per quanto riguarda l'elaborazione dei **dati personali**, come dimostrato dal recente episodio che coinvolge **Chat GPT** e l'Autorità di vigilanza italiana. L'Autorità italiana ha spiegato che Open AI non ha fornito alcuna informazione agli utenti e ai soggetti interessati i cui dati sono stati raccolti e, cosa più importante, dall'indagine dell'Autorità è emerso che "non c'era alcuna base giuridica alla base della massiccia raccolta e elaborazione di dati personali al fine di 'addestrare' gli algoritmi su cui si basa la piattaforma". Per questi motivi, l'Autorità italiana ha imposto una limitazione temporanea immediata alla disponibilità di Chat GPT per gli utenti italiani e di conseguenza all'elaborazione dei loro dati da parte di OpenAI.

Anche se non è certo come le autorità di vigilanza degli altri Stati membri reagiranno all'adozione di questa misura, d'altra parte, questo mette perfettamente in evidenza che il funzionamento dei sistemi di machine learning può essere molto controverso e sta anche dando prova del motivo per cui sia le istituzioni nazionali che europee stanno concentrando la loro attenzione sulla questione.

Per questi motivi, è responsabilità sia delle industrie che delle istituzioni pubbliche condividere informazioni su come funzionano i sistemi di apprendimento. Ciò contribuirà a creare conoscenza sull'argomento, consentendo alle persone di fidarsi dell'intelligenza artificiale e di utilizzarla a proprio vantaggio nel modo migliore possibile.

Il prossimo passo sarà l'approvazione della cosiddetta **legge sull'intelligenza artificiale**.

Avv. Aurora Agostini

aurora.agostini@lexia.it

(+39) 02 3663 8610

Dott.ssa Jessica Giussani

jessica.giussani@lexia.it

(+39) 02 3663 8610

www.lexia.it

Via del Lauro, 9 20121 Milano

Follow us on LinkedIn: <https://www.linkedin.com/company/lexia-avvocati/>