Intelligenza artificiale, cos'è, come funziona e le applicazioni in Italia ed Europa

La strategia UE sull' intelligenza artificiale è orientata a una cooperazione tra i Paesi, per favorire lo sviluppo tecnologico attraverso intervento dei governi che comprenda anche accesso ai dati pubblici e supporto al settore con investimenti, nel contempo incentivando confronto su regole di salvaguarda esseri umani. (Fonte: https://www.agendadigitale.eu/)

In Europa le iniziative dell'Unione sull'intelligenza artificiale si può dire che siano iniziate con la sottoscrizione da parte dei I **25 Paesi membri dell'Unione Europea** di una dichiarazione congiunta con cui si sono impegnati a coordinare gli sforzi nell'implementazione di sistemi di intelligenza artificiale, focalizzando l'impegno di condividere le *best practice* nel settore pubblico, di impegnarsi a rendere maggiormente disponibili i dati pubblici, di contribuire a rendere sostenibili ed attendibili le soluzioni, di assicurare la centralità dell'individuo nel loro sviluppo e di favorire lo scambio di opinioni circa gli impatti di queste tecnologie nel mercato del lavoro.
Prima di tale dichiarazione era stata lanciata call dalla Commissione Europea per la costituzione di un gruppo di esperti di alto livello sull'intelligenza artificiale e presentato il report francese sulla strategia del Paese in tale settore, che annunciava investimenti per 1,5 miliardi di euro, nonché il libro bianco pubblicato da AgID sull'adozione di soluzioni di intelligenza artificiale nell'ambito della pubblica amministrazione.
Nel 2019 sono state quindi pubblicate dal Gruppo di alti esperti europeo le Linee Guida sugli Orientamenti etici per un'IA affidabile e nel 2020 la Commissione Europea ha presentato le linee strategiche per gli anni a venire con la volonta di assicurare un ruolo all'Unione Europea

nell'ambito delle tecnologie digitali (disegnando alcune linee di azione, contenute nella comunicazione **COM(2020) 67 final**),
Ad aprile 2021 è stata presentata la proposta di **AI Act**, ossia di regolamento volto a disciplinare i sistemi di intelligenza artificiale, primo atto normativo di questo genere nel mondo.
Nel frattempo, dai primi mesi del 2023 si sta assistendo ad un'esplosione di servizi online basati su modelli generativi, sia testuali (**ChatGPT** di OpenAI in primis) sia grafici (Midjourney, Stable Diffusion e DALL-E) i quali hanno, per così dire, alzato i livelli di attenzione da parte dei regolatori.
L'intelligenza artificiale sta quindi entrando sempre di più nella nostra vita di tutti i giorni e l'Europa e tutto il mondo si preparano alle sfide e complessità che l'intelligenza artificiale porta con sé.
Ma prima di vedere come Europa, Usa e Cina si stanno "sfidando" a suon di ricerca sull'AI (Artificial Intelligence), è meglio approfondire e capire più da vicino che cos'è e come funziona l'intelligenza artificiale.

Indice degli argomenti

- Cos'è e come funziona l'Intelligenza Artificiale
- Ambiti applicativi dell'intelligenza artificiale per lavoro e società in Italia e nel mondo
- Esempi di intelligenza artificiale
    - Google Duplex, Assistente AI chiama parrucchiere e prenota
- Boston Dynamics e il robot Atlas
- Sophia, robot umanoide e AGI (Artificial General Intelligence)
- ChatGPT, Midjourney, DALL-E, Stable Diffusion ed I modelli generativi
- Intelligenza artificiale in Europa, Usa e Cina: la sfida
- Intelligenza artificiale in Europa (e in Italia)
- GDPR, privacy e intelligenza artificiale

Cos'è e come funziona l'Intelligenza Artificiale

L'intelligenza artificiale è fondamentalmente un insieme di algoritmi. Un robot, un software che gli sviluppatori cercano di rendere "intelligente", ovvero capace di imparare dai suoi stessi errori, e crescere e migliorare, apprendendo.
Secondo **Wikipedia**, si definisce come intelligenza artificiale:
«L'intelligenza artificiale (o IA, dalle iniziali delle due parole, in italiano) è una disciplina appartenente all'informatica che studia i fondamenti teorici, le metodologie e le tecniche che consentono la progettazione di sistemi hardware e sistemi di programmi software capaci di fornire all'elaboratore elettronico prestazioni che, a un osservatore comune, sembrerebbero essere di pertinenza esclusiva dell'intelligenza umana.» (**Marco Somalvico**)

In pratica si sta cercando di ricreare artificialmente l'intelligenza tipica dell'essere umano. Che vuol dire?
Ogni essere umano apprende, grazie all'intelligenza.
L'apprendimento, se ad esempio devo imparare a compiere un'azione e accrescere le mie capacità in quell'azione, consiste nel ripetere l'azione molte volte, commettere errori e imparare dagli errori che si commettono e dall'esperienza.
Con l'intelligenza artificiale si cerca di fare proprio questo. Di creare degli algoritmi che, attraverso **loop e iterazioni** possano ripetere un'azione più volte, apprendere dagli errori, e quindi imparare sempre di più a fare quell'azione. Se ad esempio ad un robot gli si chiede di giocare in continuazione a scacchi, e di imparare dagli errori. egli inizierà ad analizzare statisticamente tutte le giocate possibili, e a capire, da tutte queste giocate e da tutte le vittorie e sconfitte un po' di più il gioco degli scacchi.
Arriverà un momento in cui la macchina supererà l'essere umano nel gioco degli scacchi, avendo appreso per tantissimo tempo tutte le mosse possibili.
Per questo l'intelligenza artificiale può essere considerata come "automazione di comportamenti intelligenti".
Recentemente, inoltre, anche tenendo conto delle recenti evoluzioni tecnologiche dei sistemi di intelligenza artificiale, il legislatore europeo sta inserendo delle distinzioni tra i "Foundation Model" ed i General Purpose AI, di cui si parlerà in seguito, tentando di proporre una disciplina che possa comprendere entrambi all'interno dell'Unione Europea.

Ambiti applicativi dell'intelligenza artificiale per lavoro e società in Italia e nel mondo

I cambiamenti che l'intelligenza artificiale porterebbe alla società sono molteplici. Molti lavori vengono già sostituiti quasi completamente dalle macchine e dall'intelligenza artificiale. "Dare intelligenza" alle macchine permetterebbe di sostituire del tutto alcuni lavori ed attività oggi svolte dall'uomo. Si pensi ad esempio ad Amazon, e ai robot che crea per gestire i propri magazzini. Oppure agli assistenti vocali nel cellulare o a casa.

Esempi di intelligenza artificiale

Ecco alcuni esempi di intelligenza artificiale applicata alla vita di tutti i giorni. Ovviamente gli ambiti applicativi dell'intelligenza artificiale nelle aziende diventano un asset fondamentale per competere. Ora che l'IA è alla portata di tutti, vediamo quindi alcuni esempi di applicazioni che sfruttano l'intelligenza artificiale.

Google Duplex, Assistente AI chiama parrucchiere e prenota

L'intelligenza artificiale dell'assistente Google duplex chiama un parrucchiere e un ristorante e prenota un appuntamento e un tavolo, senza che dall'altro lato del telefono si capisca che c'è un robot.

Google Duplex: A.I. Assistant Calls Local Businesses To Make Appointments

Boston Dynamics e il robot Atlas

Boston Dynamycs (che all'epoca era stata acquisita da Google) crea robot che sfruttano sistemi di intelligenza artificiale (oltre che riconoscimento facciale, sensori di movimento e molto altro) per creare robot estremamente agili e programmati per fare varie attività, tra cui salti capriole all'indietro.

What's new, Atlas?

Sophia, robot umanoide e AGI (Artificial General Intelligence)

Sophia è un robot umanoide creato da Hanson Robotics che sfrutta l'AI di Singularity, una startup che vuole creare **AGI** (artificial general intelligence).

L'IA generale trova automaticamente modelli e caratteristiche all'interno delle informazioni senza alcun pregiudizio pre-programmato, e impara e categorizza nuovi modelli man mano che vengono rilevati fornendo output di diverso tipo e non strettamente legati ad uno specifico compito per cui è creata.

Questa proprietà non predeterminata dell'IA generica può avere un'importanza critica nelle applicazioni di sicurezza. Ad esempio, è impossibile per un terrorista o un criminale aggirare l'IA generica sapendo cosa sta cercando, poiché il sistema non ha regole pre-programmate.

Meet Sophia: The first robot declared a citizen by Saudi Arabia

ChatGPT, Midjourney, DALL-E, Stable Diffusion ed I modelli generativi

Dall'inizio del 2023 abbiamo assistito ad una vera e propria esplosione di applicazioni di intelligenza artificiale resi disponibili agli utenti online. Si tratta, in particolare, di modelli generativi che, nell'ambito di uno specifico dominio (testo, immagini, audio) consentono agli utenti di inserire delle richieste (i "prompt") ed ottenere uno specifico testo, codice sorgente, immagine che scaturisce dalla richiesta. Questi modelli sono detti "generativi" proprio perché generano in autonomia il contenuto richiesto dall'utente ed hanno ricevuto sempre più attenzione tra il pubblico per le impressionanti capacità di realizzare prodotti digitali. Si pensi che ChatGPT, il **chatbot** generativo creato da OpenAI utilizzando il Latrge Language Models (**LLM**) GT3 e GPT4, in solo due mesi dal lancio nel gennaio 2023 ha raggiunto i 100 milioni di utenti (paragonato a TikTok che per arrivare a tale traguardo ha messo 9 mesi dal lancio, o Instagram che ha impiegato 2 anni e mezzo).

La rapida esplosione di queste nuove applicazioni ha anche portato ad un intervento del Garante per la protezione dei dati personali, che ha sottolineato alcune incongruenze ed aree a rischio nel trattamento dei dati personali che viene svolto dalle stesse.

Intelligenza artificiale in Europa, Usa e Cina: la sfida

È noto che in questo settore tecnologico oggi l**a grande sfida si pone tra gli Stati Uniti e la Cina, paesi in cui si stanno diffondendo sempre più applicazioni concrete di utilizzo, sia nel settore pubblico sia in quello privato, con approcci però profondamente diversi.**

Gli **statunitensi**, fedeli alla politica liberale ed alla tradizione di *common law*, danno ampio spazio alla ricerca privata, anche mediante commesse pubbliche affidate ad aziende, mentre un ruolo assai minore ricopre l'intervento pubblico. La ricerca e sviluppo nel settore tecnologico è sostanzialmente nelle mani delle grandi società di servizi che tutti conosciamo ed i problemi etici, politici e legali sono affrontati solo in seguito ad istanze precise da parte dei gruppi di interesse.

Vero è, d'altra parte, che negli Stati Uniti il dibattito coinvolge numerosi soggetti, che hanno anche la capacità di mobilitare l'opinione pubblica, e che sul tema dell'intelligenza artificiale, ma soprattutto dei risvolti delle decisioni automatizzate, vi sono da tempo movimenti di opinione che fanno pressione per l'adozione di specifiche regole (ad esempio, in 22 Stati si è riusciti a far adottare un divieto di utilizzo dei dati relativi all'affidabilità creditizia ai fini della valutazione di canditati a posti di lavoro).

Ultimamente, in conseguenza della diffusione dei modelli generativi di cui abbiamo accennato prima, anche negli Stati Uniti sta emergendo un dibattito specifico circa la necessità di tutelare il copyright nella fase di addestramento dei modelli. Microsoft, Github ed OpenAI infatti sono stati oggetto di una class action, non ancora conclusa al momento in cui scriviamo, relativamente al tool "Copilot", ossia ad un sistema generativo addestrato con milioni di righe di codice sorgente (spesso tratto dai repository di Github) che le avrebbe utilizzate senza rispettare gli accordi di licenza con cui venivano rese disponibili.

Anche i modelli grafici come Stable Diffusion e Midjourney sono stati citati per aver utilizzato senza alcuna licenza e violando il copyright, milioni di immagini di artisti disponibili on-line.

D'altra parte ciò che emerge è che gli Stati Uniti stanno assumendo una posizione di dominio nel settore delle applicazioni di intelligenza artificiale.

La **Cina**, d'altro canto, sta adottando un approccio pilotato centralmente. L'estate del 2018 il governo cinese ha lanciato la sfida di voler fare del Paese il centro mondiale di innovazione nel settore dell'intelligenza artificiale entro il 2030. A queste parole è seguito un incremento degli investimenti pubblici e negli ultimi anni il numero di brevetti depositati da scienziati cinesi in relazione a tecnologie di intelligenza artificiale è cresciuto del 200% (in applicazioni che coprono l'intero spettro tecnologico, dai chip agli algoritmi). Il governo cinese fa ampio uso delle tecnologie di riconoscimento facciale (recentemente la società cinese SenseTime ha chiuso un round di finanziamento per 600 milioni di dollari, in cui hanno partecipato oltre ad Alibaba anche fondi statali) che vengono utilizzate per applicazioni di sorveglianza in ambito di sicurezza e prevenzione dei reati. L'intelligenza artificiale cinese, inoltre, può contare su un numero impressionante di dati da analizzare (si stima che il numero di cittadini online si aggiri su una cifra

intorno ai 750 milioni di persone) visto che ogni applicazione (Baidu, WeChat Taobao, Didi, QQ.com (gestito da Tencent)) conserva e gestisce i dati di tutti i suoi utilizzatori e, per la sostanziale inesistenza di regole a tutela della privacy dei cittadini, può facilmente condividere tali informazioni sia con le autorità governative sia con gli altri attori.
D'altra parte se anche il governo cinese sembra voler intervenire per regolare i sistemi generativi testuali (imponendo che non debbano fornire output contrari al pensiero governativo) bisogna considerare che la Cina è il paese più avanzato nella ricerca per l'applicazione dei sistemi di intelligenza artificiale nel settore della robotica (d'altronde ciò non stupisce data la rilevanza del settore manifatturiero in Cina).

Intelligenza artificiale in Europa (e in Italia)
In questo quadro si introduce l'Europa, ponendo l'accento non solo sul punto di vista tecnologico, ma anche etico, sociale e legislativo.
La via europea è, come nella tradizione del Vecchio Continente, **orientata ad una cooperazione interstatale tra i Paesi, improntata a favorire lo sviluppo tecnologico attraverso un intervento mirato dei governi che comprenda anche l'accesso ai dati pubblici ed il supporto al settore con investimenti, nel contempo incentivando il confronto sulle regole di salvaguardia per un'intelligenza artificiale "umanocentrica".**
L'attenzione alle esigenze della persona e l'equilibrio tra intervento pubblico ed autonomia privata è ciò che caratterizza da sempre la politica europea in tema di nuove tecnologie e, nello specifico, di intelligenza artificiale.
Nella **Risoluzione del Parlamento del 16 febbraio 2017** recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, in cui sono presi in considerazione anche i sistemi di intelligenza artificiale, l'Europa aveva già indicato come temi di attenzione quelli relativi ai risvolti etici e sociali, sottolineando che lo sviluppo della robotica e dell'intelligenza artificiale dovrebbe mirare ad integrare le capacità umane e non a sostituirle.
La citata Risoluzione, pur essendo tesa a fornire delle linee guida in ambito civilistico, in realtà offriva numerosi spunti su cui siamo chiamati a riflettere in un'ottica di diffusione di tecnologie intelligenti.
Tali temi, sono stati poi ripresi dal Gruppo di lavoro di alti esperti, con le Linee Guida etica per lo sviluppo di sistemi di intelligenza artificiale affidabili ed "umanocentrici" e dai provvedimenti normativi che sono stati proposti dalla Commissione Europea.
In particolare, l'AI Act, ossia la proposta di Regolamento europeo sui sistemi di intelligenza artificiale, intende proporre il primo quadro giuridico al mondo per disciplinare tali applicazioni, introducendo, nell'ambito della disciplina generale dei prodotti, un approccio basato sul rischio definendo i sistemi di intelligenza artificiale sulla base di 4 categorie di rischio: a) Inaccettabile (i sistemi di sorveglianza massiva basati su dati biometrici o i sistemi di social scoring); b) alto rischio;

c) rischio limitato; d) rischio minimo o nullo. E' interessante notare che il livello di rischio non viene valutato sulla base delle caratteristiche intrinseche del sistema (come sarebbe normale in una normativa volta a disciplinare l'immissione in commercio di prodotti), ma sono presi in considerazione gli ambiti di utilizzo in cui vengono introdotti i sistemi di intelligenza artificiale (infrastrutture critiche, scuola e formazione, sicurezza dei prodotti, rapporti lavorativi, servizi essenziali, sicurezza pubblica, migrazione ed amministrazione della giustizia).
In presenza di sistemi di intelligenza artificiale vengono introdotte delle garanzie (come sistemi di audit e certificazione, requisiti di qualità dei dati di addestramento, etc.) che devono essere attuate prima dell'immissione in commercio del prodotto.
Parallelamente all'AI Act la Commissione Europea ha proposto, a settembre 2022, l'adozione di una direttiva per adeguare le norme sulla responsabilità civile extracontrattuale all'intelligenza artificiale, la quale è strettamente collegata all'AI Act introducendo alcune presunzioni di colpa, in senso oggettivo, soprattutto con riferimento alla commercializzazione dei sistemi di AI ad alto rischio.
Come si è accennato sopra, recentemente sono state proposte delle modifiche all'AI Act per introdurre una disciplina dei Foundation Model e dei General Purpose, anche per introdurre una maggior accuratezza e qualità dei dati che sono inseriti per l'addestramento dei modelli di intelligenza artificiale.
Sembra quindi che la sfida che l'Europa dovrà affrontare per proporsi come esempio da imitare per gli altri attori (in primis USA e Cina) sarà proprio quella di riuscire in futuro a coniugare la tradizione umanistica europea (su cui si fondano i diritti fondamentali accolti dalla Carta Europea dei Diritti dell'Uomo) che sono recepiti nell'impianto normativo sopra descritto con la spinta tecnologica e omologatrice che gli strumenti di intelligenza artificiale possono comportare e, soprattutto, con le sempre maggiori tendenza autonomiste che le due superpotenze stanno assumendo anche, e soprattutto, per motivi di geopolitica internazionale..

GDPR, privacy e intelligenza artificiale

Il tentativo di regolare ed assicurare l'*accountability* dei sistemi, necessita della trasparenza delle scelte che vengono fatte dagli algoritmi (ad esempio, con appositi diritti come il "*right of explanation*" citato nel considerando 71 del Regolamento (UE) n. 679/2016 (GDPR) e poi non disciplinato nel testo normativo), dell'istituzione di sistemi di tracciatura di ogni scelta effettuata dal sistema, in modo da poter renderla trasparente, della costruzione di modelli statistici, su cui opera l'intelligenza artificiale, che assumano quale componente fondamentale l'acquisizione del *feedback* sulle scelte compiute, così da poter effettuare migliori decisioni in futuro.
Oltre al tema della trasparenza del sistema anche quello dei dati che sono trattati dallo stesso assume un'importanza primaria. È noto che in informatica vige il detto "*garbage in, garbage out*"

ed in quest'ottica la qualità e pertinenza del dato su cui un sistema di intelligenza artificiale opera le proprie scelte incide in maniera fondamentale sull'esito delle stesse.
È così necessario che tali sistemi, specialmente se utilizzati per assicurare l'ordine pubblico e la sicurezza sociale, evitino di fondare le proprie valutazioni su dati non attinenti alla singola persona e che possano avere conseguenze sulla stessa (come valutazioni in base al luogo di residenza, al comportamento della comunità, etc.).
Nel provvedimento che il Garante per la protezione dei dati personali aveva adottato nei confronti di ChatGPT a marzo 2023 lo stesso aveva evidenziato alcune problematiche, tra cui assumono rilevanza particolare quella dell'assenza di un'idonea base giuridica per il trattamento dei dati personali a scopo di addestramento del modello e il mancato rispetto del principio di esattezza dei dati di cui all'art. 5 del **GDPR**, dato che in alcuni casi i modelli generativi forniscono *output* con informazioni inesatte su persone specifiche.
Il tema ha assunto rilevanza in Europa, e l'European Data Protection Board ha costituito una *task force* al proprio interno proprio al fine di affrontarlo in maniera adeguata.
Sicuramente in Unione Europea è stata sin dall'origine sottolineata la delicatezza e l'importanza dei dati nell'addestramento di tali sistemi, soprattutto cercando di incentivare la creazione di banche dati pubbliche europee (si veda il Data Governance Act) eliminando così il *gap* che esiste in Europa circa la disponibilità di informazioni da utilizzare per addestrare sistemi di intelligenza artificiale.
Rendere disponibili tali dati ai soggetti privati che implementano soluzioni di intelligenza artificiale incentiverebbe tali attività, dato che i sistemi di ***machine learning*** devono processare ingenti quantitativi di informazioni per poter essere opportunamente istruiti. Però rendere accessibili pubblicamente tali dati, senza opportune misure e cautele, potrebbe avere delle conseguenze negative sulle persone. Si pensi ai dati sanitari, che potrebbero essere utilizzati per sviluppare sistemi di intelligenza artificiale in campo medico per la prevenzione delle malattie (già oggi realizzati), ma al contempo utilizzati per altre finalità, ad esempio per negare l'accesso a posti di lavoro o per negare coperture assicurative.
Siamo convinti che l'Europa potrà assumere un ruolo importante nel settore dell'intelligenza artificiale se rimarrà fedele ai principi etici ed umanistici su cui si fonda, fornendo l'esempio di come la tecnologia debba porsi al servizio delle persone, in un'ottica, si ripete, "umano-centrica".