White Paper
L'IA in azione

A cura del
Gruppo di lavoro "intelligenza artificiale"
di Anitec-Assinform

Ottobre 2023

Anitec-Assinform

Anitec-Assinform

Realizzato da:

Anitec-Assinform, gruppo di lavoro "Intelligenza artificiale". Coordinatore: Roberto Saracco (Reply).

Hanno contribuito le aziende associate:

Cefriel, Colin & Partners, DXC, Engineering, Eustema, Experis, Exprivia, IBM, Indra Minsait, Leonardo, Maxfone, Microsoft, Mylia, Reply, TIM.

Si ringrazia inoltre:

AINDO.

I dati nella parte due sono stati forniti da NetConsulting cube.

Anitec-Assinform

Sommario

EXECUTIVE SUMMARY

Il White Paper "l'IA in azione" è il terzo prodotto dal Gdl Intelligenza artificiale di Anitec-Assinform. I primi due documenti si sono concentrati sulle opportunità offerte dall'IA per la ripresa dell'economia dopo la crisi pandemica[1] e sull'approfondire il contesto tecnologico, regolatorio e competitivo nel quale l'IA sta venendo sviluppata in Italia e nel mondo[2].

Nel mondo post-pandemico, le imprese si trovano a dover affrontare sfide globali senza precedenti, tra cui la sostenibilità e la resilienza delle supply chain. Questo scenario è caratterizzato da un'evoluzione tecnologica rapida che include lo sviluppo e la diffusione di tecnologie come: l'Internet of Things, il Cloud Computing fino al Quantum Computing. Il cambiamento tecnologico offre nuove opportunità di business ma crea anche domanda di nuove competenze. In questo contesto, il potenziale dell'IA è indiscutibile, specie pensando ai recenti sviluppi nell'ambito dell'IA generativa. Tuttavia, c'è una distonia significativa tra ciò che la tecnologia può offrire e il suo utilizzo effettivo nel panorama produttivo italiano.

Secondo la nostra analisi, questo divario è principalmente dovuto alla mancanza di comprensione della tecnologia, alla difficoltà nel trovare competenze adeguate e a una cultura aziendale e manageriale non sempre pronta ad accogliere il cambiamento.

Il White Paper offre al lettore anche una fotografia dello stato attuale e delle prospettive future, del mercato delle soluzioni di IA in Italia. Nel 2023, il mercato italiano dell'IA dovrebbe raggiungere i 570 milioni di euro. Nonostante una penetrazione ancora limitata, soprattutto nelle PMI, il mercato è previsto crescere mediamente quasi del 30% annuo, toccando 1,2 miliardi di euro nel 2026. I settori bancario e delle telecomunicazioni/media sono i più attivi negli investimenti in IA, mentre la pubblica amministrazione è più indietro. Le tecnologie che stanno guadagnando maggiore attenzione riguardano l'Intelligent Data Processing, il Natural Language Processing e la creazione di Chatbot.

Questo avviene in un contesto regolatorio europeo ancora in fase di definizione, che sembra concentrarsi più sui possibili rischi associati all'IA piuttosto che sulle opportunità

[1] Anitec-Assinform. Promuovere lo sviluppo e l'applicazione dell'Intelligenza artificiale a supporto della ripresa". 2021.
[2] Anitec-Assinform. "L'IA a tre dimensioni, approfondimenti su policy, tecnologie ed esperienze aziendali". 2022.

che può offrire. Riteniamo, in questa sede, che sia importante dare risalto alle molteplici possibilità che l'IA può offrire, soprattutto per le piccole e medie imprese (PMI), al fine di promuovere una adozione più ampia e consapevole di questa tecnologia.

Il White Paper si rivolge in primo luogo a tutti coloro che sono curiosi di approfondire il tema dell'introduzione dell'IA nei modelli di business aziendali, offrendo un testo ricco di contenuti tecnici resi in modo accessibile e mutuati dall'esperienza delle aziende dell'ICT che operano in Italia. In secondo luogo, il White Paper si rivolge agli stakeholder istituzionali, coloro i quali sono chiamati "saper maneggiare" sempre meglio la tecnologia. Il testo offre ai decisori pubblici punti di vista e spunti da parte dell'Industria ICT sulle traiettorie di sviluppo dell'IA e l'impatto che la tecnologia avrà su economia e società.

Lanciamo con questo White paper una *call to action*: per restare competitivi abbiamo bisogno di più IA nelle nostre aziende, di skills più vicine alle necessità dell'industria, di un contesto regolatorio che tenga conto delle esigenze degli innovatori e di un rinnovamento nella cultura manageriale delle nostre aziende.

Il testo è strutturato come segue: la prima parte affronta il tema della tecnologia, evidenziando come per lo sviluppo dell'IA si parta dalle sorgenti dei dati per poi generare valore da essi. La seconda parte offre *insights* sulle dinamiche di mercato dell'IA in Italia, la terza parte raccoglie best practices e *use case* raccolti da numerose aziende associate ad Anitec-Assinform, la quarte parte presenta degli scenari applicativi su diversi settori verticali.

INTRODUZIONE

Il Gruppo di Lavoro "intelligenza artificiale" di Anitec-Assinform ha prodotto negli ultimi due anni due White Paper; il primo "Promuovere lo sviluppo e l'applicazione dell'intelligenza artificiale a supporto della ripresa", sviluppato in piena pandemia e con un contesto in forte cambiamento (remotizzazione di attività, automazione, ecc…), il secondo, "L'IA a tre dimensioni. Approfondimenti su policy, tecnologie ed esperienze aziendali" per collocare l'adozione di questa tecnologia in un contesto mondiale che presenta forti differenze nelle traiettorie di regolazione che andranno a incidere sempre più profondamente sull'adozione dell'IA e sulle sue opportunità di sviluppo.

Superata la fase pandemica, sono molte le aziende che cercano di ripristinare la "normalità", pur in presenza di nuove criticità a livello globale che impattano il contesto operativo e competitivo. Altre aziende, invece, portano avanti le scelte indotte dalla pandemia, rivedendo processi e strumenti.

Oggi, tutte le imprese devono confrontarsi con un mercato che in pochi anni è profondamente mutato. È imperativa una maggiore attenzione alla sostenibilità così come la prioritizzazione della resilienza delle *supply chain*. Efficienza e flessibilità in un contesto di riduzione dei consumi energetici devono andare di pari passo pur essendo, in alcuni casi, in opposizione l'uno con l'altro.

Allo stesso tempo, l'evoluzione tecnologica complessiva – dall'IoT (Internet of Things) sempre più pervasive e "smart" al trattamento dei dati (cloud, security, privacy, processing con il quantum computing in crescita) e della loro interpretazione e visualizzazione (analytics, Intelligenza artificiale in the large e in the small, realtà aumentata e realtà virtuale/metaverso) offre, da un lato, nuovi strumenti all'impresa, e dall'altro sottolinea l'allargarsi di uno *skill-gap* che deve essere affrontato con nuove risorse e metodologie.

Le proposte europee sul Data Act e su AI Act si stanno consolidando, così come azioni legislative a livello nazionale facendo evolvere il quadro normativo. Attenzione crescente, in questo contesto, viene rivolta agli aspetti etici e sociali legati ad un uso sempre più pervasivo dei dati.

A livello dell'evoluzione dell'Intelligenza artificiale, vista come insieme di tecnologie, riveste particolare importanza – sia per l'hype generato sia per le concrete possibili applicazioni aziendali in termini di efficientamento e offerta servizi – l'area della **Generative AI**. Questa non è una novità assoluta in

termini tecnologici (le GAN, Generative Adversarial Network che rappresentano il progenitore di questa tecnologia sono state introdotte nel 2014 mentre i transformer appaiono nel 2017) ma lo è in termini di utilizzabilità. A livello globale, con il rilascio della famiglia GPT -GPT-3 e l'interfaccia conversazionale ChatGPT- nello scorso anno e quella del GPT-4, Bard e LLaML (rispettivamente di Open AI, Google e Meta) nei primi mesi del 2023.

È da rimarcare la rapida presa di consapevolezza sul potenziale impatto sull'operatività aziendale e sulle modalità di interazioni con i clienti di queste nuove tecnologie che ha portato allo sviluppo in termini rapidissimi di corsi da parte di diverse università per formare nuovi profili in grado di utilizzarle.

Questo è interessante anche perché sottolinea, come la Generative AI non sia una rivoluzione in sé ma piuttosto uno strumento molto potente che, se utilizzato in modo opportuno e integrato nei processi aziendali, può portare ad un aumento della produttività (da alcuna osservatori stimato tra il 5 e il 25% a seconda dei settori)[3].

In linea di massima, l'IA generativa, si presta a essere utilizzata bene o male e la responsabilità dovrebbe essere a carico dell'utilizzatore. È da notare come i LLM (Large Language Model) siano il risultato dell'accesso a dati da parte di grandi aziende come Google, Meta, o Microsoft che li mettono a disposizione attraverso interfacce Web e API in termini di servizi (più o meno gratuiti). Questi dati hanno una valenza generale, non sono specifici di una realtà/interesse aziendale. Proprio in questi ultimi mesi, tuttavia, stanno emergendo strumenti che consentono di affiancare a questi LLM dei modelli di dati molto più piccoli ma focalizzati a specifiche realtà, consentendo quindi a una azienda di creare il proprio "spazio dati" su cui utilizzare la Generative AI.

A quest'evoluzione corrisponde una **crescente adozione della IA classica (non Generative) nel contesto delle imprese e da qui la decisione del Gruppo di Lavoro di dare, attraverso questo WP, una fotografia aggiornata dell'uso, del contesto e delle sfide e opportunità per le aziende italiane.**

Al tempo stesso questa "testimonianza" di aziende, arricchita anche attraverso i contatti diretti con il territorio conseguenti al Roadshow organizzato da Anitec-

[3] Si veda, ad esempio, lo studio di McKinsey "The Economic Potential of Generative AI" https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#introduction

Assinform e Confindustria può rappresentare un valore per il legislatore italiano nell'affrontare questi temi.

1. Parte prima – Evoluzione del contesto tecnologico

L'IA evolve sempre più rapidamente. Come mai?

Il progresso tecnologico è continuo, praticamente in tutti i settori. Tuttavia, nel contesto dell'intelligenza artificiale quest'evoluzione ha caratteristiche esponenziali così come è stato nel settore dell'elettronica con l'evoluzione dei chip. Quest'ultima, infatti, ha beneficiato del feedback sul processo di sviluppo e realizzazione dei chip:

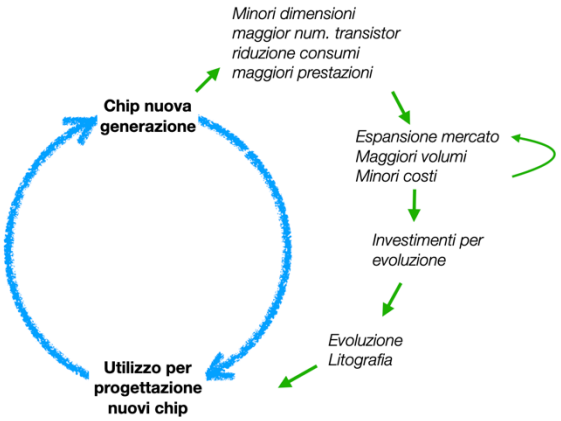


Figura 1. Il ciclo virtuoso che ha portato al progresso nel settore della microelettronica. Il nuovo chip prodotto viene utilizzato anche dal processo di produzione di chip che sfruttando le migliori performance riesce a produrre chip ancora migliori.

In altre parole, ciò che si è osservato è stato:

1. sviluppo di chip di nuova generazione (riduzione delle dimensioni del gate, riduzione consumi, aumento prestazioni)
2. utilizzo dei nuovi chip (maggiori prestazioni) per la progettazione di chip di nuova generazione
3. miglioramento delle tecniche litografiche
4. minori costi e quindi espansione del mercato e crescita della domanda a giustificare nuovi investimenti nella produzione

Per l'Intelligenza artificiale il ciclo è più articolato ma porta alle stesse conseguenze di crescita esponenziale:

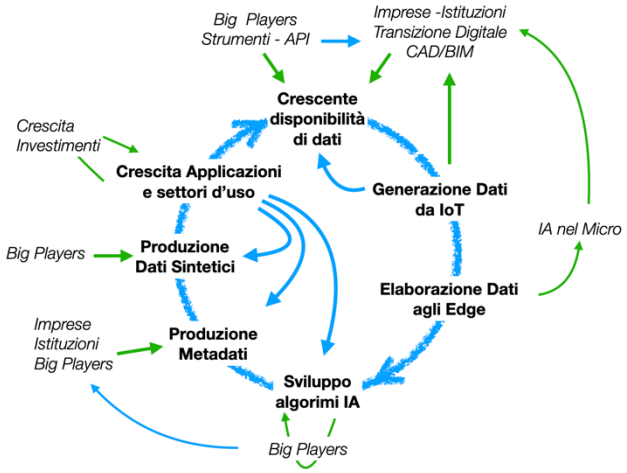


Figura 2, L'evoluzione della IA è in questa fase guidata dai dati. Questi sono sempre più numerosi e grazie a capacità elaborative sempre maggiori riescono a migliorare il livello di intelligenza. A sua volta questo porta ad un maggiore utilizzo della iA che genera ulteriori dati e porta ad un rapido miglioramento del livello di intelligenza. Si noti come anche le imprese, piccole e grandi, adottando la IA nei loro processi diventino "produttori" di IA.

1. Crescente disponibilità di dati, sia a livello "macro" - grandi basi dati -, sia a livello di imprese che di istituzioni, in conseguenza della transizione digitale e dell'adozione di progettazione digitale.
    a. A livello macro l'evoluzione porta alla creazione di strumenti, sempre più potenti, che consentono a una molteplicità di attori, incluse le imprese di utilizzare l'IA
    b. A livello micro l'utilizzo di dati storici per machine learning
2. Incremento del numero di sensori IoT, che generano importanti flussi di dati a livello dei sistemi produttivi ed *embedded* nei prodotti (con flusso dai prodotti al sistema di monitoraggio uso e qualità in ottica industria 4.0)
3. Disponibilità crescente di sistemi di elaborazione agli edge con preelaborazione dei dati (IoT gateways)
4. Sviluppo di algoritmi di IA e recente evoluzione della *generative AI*
5. Produzione di metadati
6. Produzione di dati sintetici

7. Incremento di applicazioni e utilizzo di IA che genera nuova domanda di IA e stimola investimento nel settore

Come siamo arrivati a questo punto

Il termine intelligenza artificiale è stato coniato negli anni '50 ma solo negli ultimi anni stiamo vedendo direttamente i benefici che derivano dalla diffusione di questa tecnologia.

In passato ci sono stati periodi di entusiasmo alternati ai cosiddetti "AI Winter", ovvero periodi di declino causati dalla mancanza di risultati concreti con conseguente calo di interesse degli investitori e del pubblico.

Rispetto al passato oggi ci troviamo però in uno scenario di euforia dettato principalmente dai seguenti motivi:

1. l'avvento di tecnologie informatiche avanzate come il cloud computing, i big data e l'IoT che hanno reso possibile l'elaborazione e la gestione di grandi quantità di dati
2. l'avanzamento delle tecniche di IA come il Machine Learning, il Deep Learning e la Generative AI hanno permesso di ottenere risultati più precisi e significativi in molti settori,
    a. a ciò va sommato che l'utilizzo di IA sempre più performanti è stato reso accessibile fino alla dimensione del singolo utente di internet, in particolare con la diffusione di applicazioni di IA generativa (es. ChatGPT, DALL-E, MidJourney etc…)

IA per le aziende

Ogni azienda oggi produce un enorme quantitativo di dati ed è proprio in questo contesto che si fa riferimento ai Big Data.

Il termine Big Data si basa su tre dimensioni:

1. Volume: la vasta quantità di dati che viene generata ogni giorno

2. Velocità: la rapidità con cui i dati vengono generati e raccolti, che richiede un'elaborazione molto spesso in tempo reale
3. Varianza: la diversità dei dati, come ad esempio diversi formati, fonti e tipologie

I dati però non bastano a produrre risultati e informazioni strategiche per ottenere un vantaggio competitivo, questi devono essere analizzati con i giusti strumenti.

È per questo motivo che termini come Big Data e Intelligenza artificiale corrono di pari passo: i Big Data senza strumenti di analisi avanzata non producono risultati e, viceversa, senza dati di alta qualità, l'IA non può funzionare correttamente o generare risultati accurati.

Le maggiori **difficoltà che le aziende di piccole e medie dimensioni si trovano ad affrontare** sono quindi da ritrovare nella **scalabilità della propria infrastruttura tecnologica**, motivo per cui molto spesso si fa affidamento al **Cloud**.

Oggi le aziende possono: da una parte, accedere a risorse di archiviazione scalabili a basso costo per i propri dati e, dall'altra parte, sfruttare potenza computazionale per lo sviluppo di modelli di intelligenza artificiale senza doversi preoccupare di investimenti frontali sull'acquisto di hardware ad alte prestazioni.

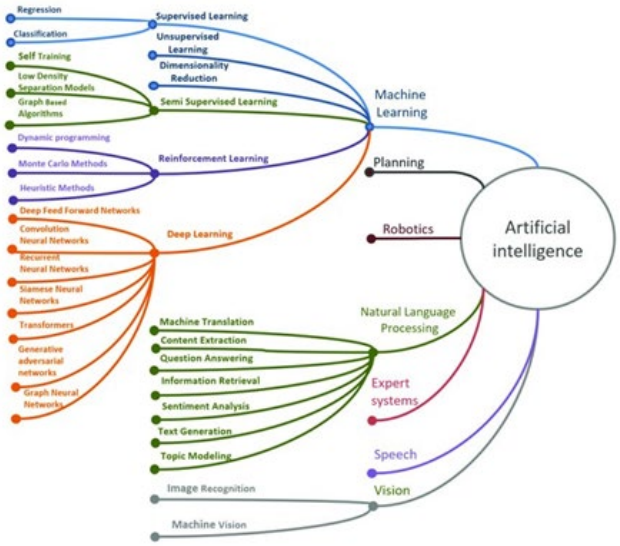


Figura 3. L' Intelligenza artificiale é un "obiettivo" che si persegue utilizzando una varietá di tecnologie, ed a seconda dei settori di applicazione, schematizzati in questo grafico, alcune tecnologie risultano piú adatte. Nel grafico, le tecnologie piú frequentemente utilizzate sono raggruppate nell'arco superiore sotto l'etichetta Machine Learning.

Le varie "sfumature" dell'IA

L'Intelligenza artificiale, quindi, rappresenta un insieme di tecniche e algoritmi che consentono a una macchina di eseguire compiti che richiedono una certa forma di intelligenza che si ritrova in quella umana, come il riconoscimento di immagini, la comprensione del linguaggio naturale, il ragionamento e la pianificazione.

Mentre nel passato si cercavano algoritmi che potessero emulare l'intelligenza umana, negli ultimi 20 anni ci si è spostati sempre più sulla possibilità di derivare comportamenti intelligenti a partire dalla analisi dei dati, anche perché diventavano disponibili enormi quantità di dati e da questi volumi era possibile estrarre significati tramite correlazione, e quindi "intelligenza". Inoltre, in molti casi, questi dati rappresentano una certa forma di intelligenza, essendo prodotti da intelligenza umana (si pensi a tutti i libri, articoli, conversazioni presenti sul Web). Alcuni settori di applicazione, come ad esempio il riconoscimento di immagine, sono ancora dominati dall'uso di tecniche algoritmiche, altri, come la traduzione in tempo reale sono quasi esclusivamente basati sui dati.

Il **Machine Learning** è una sottocategoria dell'IA che si concentra sull'abilità delle macchine di apprendere dai dati senza essere esplicitamente programmate. In altre parole, le macchine sono in grado di acquisire conoscenze tramite l'analisi di grandi quantità di dati e di utilizzare queste conoscenze per fare previsioni o prendere decisioni.

Il **Deep Learning** è una tecnica di Machine Learning che cerca di simulare il funzionamento del cervello umano tramite l'uso di una **rete neurale artificiale** composta da molti strati di neuroni. Ciò consente alle macchine di apprendere direttamente dai dati, invece di dover affidarsi all'estrazione manuale di caratteristiche. Grazie alla capacità di apprendimento autonomo di queste reti neurali, **il Deep Learning viene di solito utilizzato per l'analisi di dati non strutturati** come immagini, testo ed audio.

La Generative AI (intelligenza artificiale Generativa) è un campo dell'intelligenza artificiale che sfrutta delle enormi basi di dati che vengono elaborati attraverso algoritmi di apprendimento automatico per generare nuovi contenuti, come immagini, suoni e testo.

Gli algoritmi usati dalla Generative AI hanno l'obiettivo di "trasformare" dati contenuti nei LLM in altri dati che probabilisticamente corrispondano ad una stringa di input (la domanda posta dall'utilizzatore). Queste tecniche vanno sotto il nome di Transformer e a loro volta si basano spesso sul Deep Learning e utilizzano tecniche come i GAN (Generative Adversarial Networks), che consentono alle macchine di generare nuovi contenuti che si avvicinano ad un obiettivo prestabilito (ad esempio vincere a scacchi o produrre una immagine che abbia certe caratteristiche).

Nel seguito si approfondiscono tutti questi elementi con particolare focus sulle sorgenti di dati, trattamento dei dati e leverage sui dati.

1.1. Sorgenti di dati

1.1.1. Introduzione

Tutto il sistema produttivo, a partire dalle risorse primarie fino a vendita, assistenza e manutenzione – ovviamente passando per la produzione di beni – utilizza e genera dati. In questo contesto, la Trasformazione Digitale incrementa ulteriormente sia la creazione di dati sia il loro flusso.

Le aziende hanno una quantità crescente di dati (generati all'interno dell'azienda o derivati da interazioni con l'esterno) di cui la maggior parte non è messa a valore. Le stime affermano che il 60/95% dei dati disponibili non sono di fatto utilizzati (questi valori sono difficili da quantificare ma il messaggio è chiaro: esiste un potenziale non sfruttato).

Il mancato utilizzo deriva, sia da una mancata percezione di una loro utilità, sia da una difficoltà oggettiva di utilizzo (vedi 1.2 e 1.3). Inoltre, **spesso i dati non sono concepiti come una risorsa ma come un *by-product* di un processo ed esauriscono il loro valore all'interno del processo stesso**. Ad esempio, i dati risultanti da sensori che monitorano il funzionamento dei torni digitali sono usati dal tornio stesso, anche se restano disponibili all'azienda. Quegli stessi dati potrebbero essere utilizzati a valle per una analisi sulle cause di deficit qualitativi del prodotto, generando quindi azioni correttive.

Inoltre, occorre notare come al momento le varie sorgenti di dati, di cui è data una breve sintesi in questo capitolo, producano dati in formati diversi non pensati per usi diversi da quelli per cui sono stati generati.

Iniziative come Gaia-X o come i Common European Data Spaces hanno l'obiettivo di promuovere la creazione di "spazi dati" che possano essere utilizzati da vari attori per diversi scopi, pur assicurandone la proprietà e riservatezza nella misura necessaria.

È opportuno che le aziende, soprattutto le PMI, "censiscano" di tutti i dati che posseggono, direttamente generati dai processi aziendali o acquisiti nelle interazioni con altri attori nella catena del valore e che si pongano l'obiettivo di sfruttarli. L'Intelligenza artificiale è uno strumento potente a questo scopo.

Data governance e sorgenti di dati

I dati rappresentano l'asset fondamentale per progettare ed allenare qualsiasi forma di Intelligenza artificiale.

La consapevolezza di questa "risorsa" è cresciuta in modo esponenziale nel corso degli ultimi anni, tanto da attirare l'attenzione di molti stakeholder, non ultimo la Commissione Europea che ha definito delle politiche specifiche dedicate all'economia dei dati.

All'interno dell'azione principale denominata European Data Governance, sono contenute delle misure regolamentari tra cui il Data Governance Act, già operativo, e altre in fase di pubblicazione come il Data Act che probabilmente verrà adottato alla fine del 2023 o nel primo semestre 2024 e che inizierà ad avere effetto dal 2025-26.

Se la consapevolezza è stata la scintilla che ha innescato questa prima fase, ora è sulla strategicità dei dati che si sta spostando l'attenzione di tutti gli attori. Di fatto, il concetto di "accesso ai dati" o meglio "neutralità di accesso ai dati" rappresenta per le imprese europee un elemento non trascurabile per essere protagonisti nell'economia dei dati, specialmente per le startup o imprese innovative. I dati, nelle varie forme, sono indispensabili per lo sviluppo di qualsiasi nuova impresa su qualsiasi mercato.

L'Europa, con molto ritardo, sta cercando di creare un'industria dei dati, che fa la "differenza" tra essere solo un mercato o essere protagonista con una propria filiera/ecosistema.

Ogni "emozione" genera dati – IOT e le esperienze delle macchine.

Esistono, in modo molto semplice, due ambiti dove vengono costantemente generati dati: l'IoT (Internet of Things), relativo alle cose, e l'IoB (Internet of Behaviors), relativo alle persone ed ai comportamenti. Quest'ultimo ambito comprende anche la gestione dei processi aziendali e le interazioni tra persone, interne ed esterne all'azienda, come le interazioni con i clienti, dirette o mediate da macchine. Spesso, questi due ambiti sono talmente vicini o combinati tra loro da generare set di dati unici. L'abitudine alla corsa, abbinata a dati personali fisici (età, sesso, altezza, scarpe, etc) e dati di performance raccolti da dispositivi IoT indossabili, offrono per ogni specifica "esperienza" un dettaglio unico.

L'impiego di questo tipo di set di dati rappresenta un'enorme opportunità sia per l'industria nello sviluppo di nuovi dispositivi sia per la creazione di nuove applicazioni. All'interno di questi due scenari esistono diverse dinamiche di mercato di cui tener conto che possono influire sullo sviluppo di soluzioni di IA.

1.1.2. Data Spaces: il mercato dei dati

Dal punto di vista tecnico/regolamentare nel volere definire un nuovo mercato per lo scambio dei dati (Platform for data sharing)[4] le due categorie di cui al punto sopra, sono state definire in modo più preciso: Industrial Data Spaces (IDS) e Personal Data Space (PDS), non solo, per sfruttare il valore dei dati a vantaggio dell'economia e della società europee, la Commissione sostiene lo sviluppo di spazi comuni europei di dati in settori economici strategici e settori di interesse pubblico.

La strategia europea per i dati del febbraio 2020 ha annunciato la creazione di spazi di dati in 10 settori strategici: sanità, agricoltura, industria manifatturiera, energia, mobilità, finanza, pubblica amministrazione, competenze, cloud europeo per la scienza aperta e conseguimento degli obiettivi del Green Deal, che rappresenta una priorità trasversale fondamentale. L'obiettivo ultimo è che gli spazi di dati nel loro insieme formino un unico spazio europeo dei dati: un vero e proprio mercato unico dei dati.

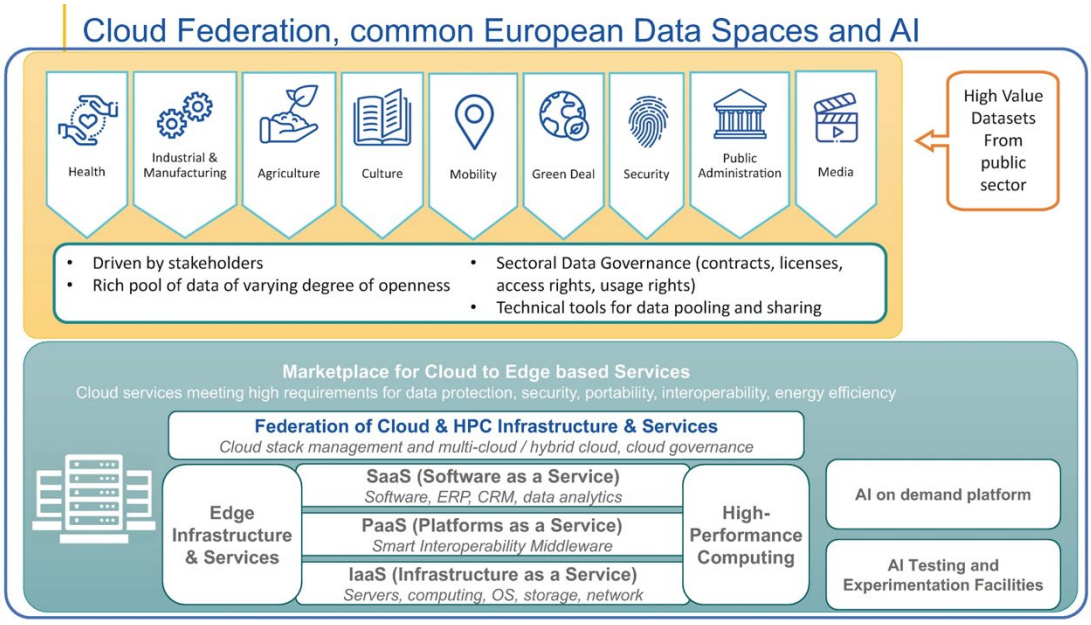


Figura 4. Rappresentazione schematica dei Data Spaces, obiettivo di standardizzazione da parte della EU per favorire lo sfruttamento dei dati da parte delle imprese. Nella parte superiore le diverse aree applicative a cui deve corrispondere un data space. Nella parte inferiore é schematizzata l'architettura di interscambio dei dati.

[4] https://link.springer.com/content/pdf/10.1007/978-3-030-93975-5.pdf?pdf=button

1.1.3. CAD

L'utilizzo del CAD -Computer Aided Design- è una realtà diffusa da diversi decenni. In questo periodo l'evoluzione è stata notevole, ovviamente, e sono molteplici i sistemi sul mercato, ciascuno con una sua propria modalità di strutture dati. Proprio per ovviare a questa diversità si sono sviluppate tecniche per assicurare l'interoperabilità (traduzione diretta tra standard proprietari, utilizzo di una rappresentazione neutra, traduzioni ad hoc effettuate da terze parti).

I dati generati da un CAD costituiscono un modello statico di una entità, un ingranaggio, un motore, …e non rappresentano il modo in cui questo "funziona". Tuttavia, questi dati sono spesso utilizzati da applicazioni il cui obiettivo è simulare il comportamento (e funzionamento) di quella entità in un certo contesto. Questi strumenti generano essi stessi ulteriori dati.

Inoltre, in svariati settori, il CAD fornisce delle librerie di componenti predefiniti (plug-in) e a questi è spesso associato un insieme di informazioni (e software) che possono essere utilizzate per simulare il comportamento di un pezzo/sistema.

Il modello generato dal CAD è il punto di partenza per la creazione del digital twin della entità (1.3.2).

1.1.4. BIM

Cosa è il BIM

Il BIM (Building Information Modelling) è una metodologia progettuale adottata nel settore AEC (Architecture, Engineering and Construction) che consente di progettare un'opera e registrarne la sua evoluzione in ciascuna delle sue fasi di vita.

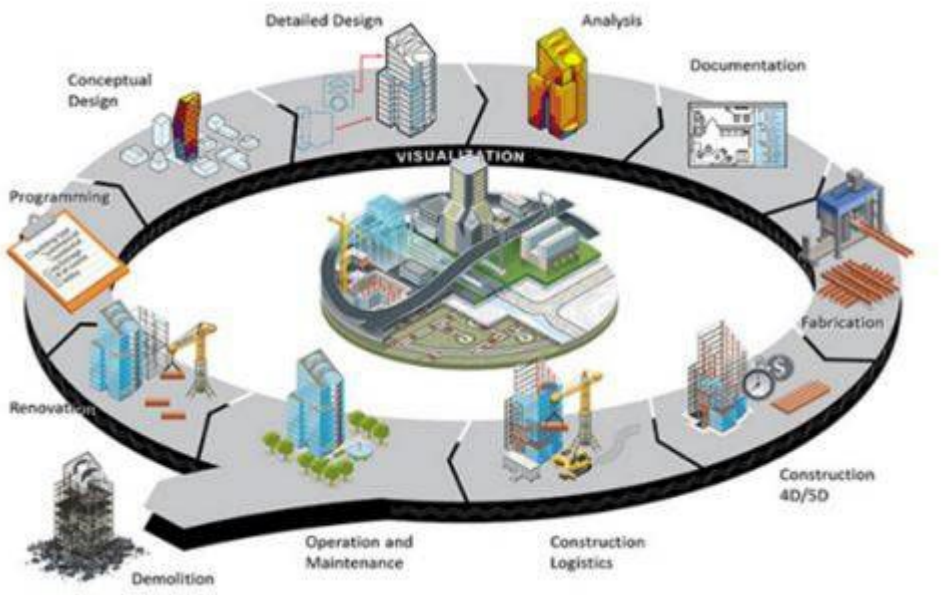


Figura 5 - BIM per il ciclo di vita dell'opera (Ingenio;2017; "Quando nasce il BIM?")

Come funziona la metodologia BIM

Un modello BIM è una rappresentazione multidimensionale di un'opera, che si compone da una rappresentazione grafica tridimensionale di ciascuno dei componenti (muro, solaio, finestra, porta, …) e dai loro specifici attributi, quali materiali, caratteristiche tecniche, caratteristiche qualitative e quantitative. Può essere creato un modello BIM per ciascuna disciplina oggetto della progettazione (strutture, impianti, architettura, …) e l'insieme di questi modelli genera il cosiddetto "modello federato".

Quando nasce il BIM

La metodologia BIM è l'evoluzione del metodo tradizionale di progettazione basato sull'utilizzo di elaborati bidimensionali CAD.

Storicamente il settore dell'architettura, ingegneria e costruzioni ha mostrato di avere bassi livelli di produttività, con enormi sprechi e ritardi, dovuti anche a una resistenza all'innovazione.

La metodologia BIM nasce come risposta a queste problematiche verso la fine del secolo scorso, ma la sua adozione si avrà solo nei primi anni 2000 grazie anche alla diffusione sul mercato dei primi software dedicati alla modellazione BIM.

In Italia l'obbligatorietà dell'adozione della metodologia BIM per gli appalti pubblici è stata introdotta con il DM 560/2017 in cui sono state definite le soglie minime di obblighi del BIM, riviste successivamente con il DM312/2021.

Perché si usa la metodologia BIM

Il BIM consente di attivare un processo di progettazione integrale, il che implica una **centralizzazione dei dati e una migliore collaborazione tra gli attori, con una complessiva mitigazione dei rischi di progetto**.

1.1.5. IoT (Internet of Things)

L'"Internet delle Cose" – IoT- è una realtà pervasiva sia nelle imprese a livello dei processi di approvvigionamento, realizzazione e distribuzione, sia a livello dei prodotti. **In massima parte le IoT sono dei sensori che rilevano parametri vari e forniscono i dati tramite collegamento alla rete**.

Gran parte dei processi aziendali si avvale di IoT per il monitoraggio degli apparati e delle attività. Questi dati rappresentano un flusso spesso importante come volumi e sono principalmente orientati ad intercettare anomalie puntuali (ad esempio un eccesso di temperatura, una mancanza di lubrificante, …). Attraverso applicazione di intelligenza artificiale questi dati possono essere analizzati per fornire analisi predittive (possibilità di intercettare potenziali problemi che possono essere risolti attraverso manutenzione preventiva prima che si manifesti un danno, possibilità di cambiare i ritmi e ribilanciare delle attività per mantenere i livelli di produzione inalterati pur diminuendo il carico su certi apparati, …).

Inoltre, questi dati diventano un elemento di apprendimento (machine learning) applicabile sia ai processi dell'azienda sia a quelli di altre aziende.

Ai dati "interni" si aggiungono sempre più spesso quelli generati dai prodotti durante il loro utilizzo (con il consenso alla raccolta da parte dell'utente). L'applicazione di IA a questi flussi di dati consentono sia di fornire servizi al cliente finale (*fine tuning* del prodotto in base all'uso effettivo, interventi di manutenzione preventiva, …) sia di "imparare" e utilizzare questa conoscenza dal campo nell'affinamento del prodotto (e del processo produttivo) per successive versioni o per la progettazione di altri prodotti.

Le IoT stanno evolvendo rapidamente in termini di capacità di generazione dati e anche di processamento locale dei dati (IoT cluster) sia attraverso software sia attraverso firmware inserito in gateways.

Un esempio di questa evoluzione è la linea STM32 di ST Microelectronics pensata per consentire elaborazioni "intelligenti" agli edge, trasferendo verso il centro di controllo una quantità inferiore di dati frutto di pre-elaborazione (metadati).

Un elemento di crescente importanza è la garanzia di affidabilità di questi dati, cioè che questi non vengano alterati da azioni di terzi. Gli aspetti di sicurezza sono fondamentali e anche qui l'IA può contribuire a rilevare possibili degradi della qualità dei dati e la possibile fonte.

1.1.6. Metadati

I dati "grezzi" generati dalla IoT, così come quelli che derivano direttamente dai vari processi sono oggetto di elaborazione e portano alla generazione di ulteriori dati. Si noti come questi dati – chiamati metadati – possano essere il risultato di elaborazioni complesse effettuate su diversi flussi (o su dati provenienti da uno stesso flusso in momenti diversi).

I metadati sono un *by-product* fondamentale della "digitalizzazione" nel momento in cui questa viene "valorizzata", cioè quando i dati che essa genera sono elaborati e danno origine a nuove informazioni. Nella prima fase di digitalizzazione in genere non viene sfruttata questa potenzialità dei dati in quanto i dati generati sono funzionali alla operatività di certi apparati. Questo è quanto porta alla enorme sottoutilizzazione dei dati citata precedentemente (dal 60 al 90% dei dati generati non viene di fatto utilizzata). Al tempo stesso

è quello che offre una grande opportunità alle aziende per migliorare i processi e i prodotti, oltre ad offrire nuovi servizi.

I metadati, quindi, sono informazioni aggiuntive o descrittive che forniscono contesto, struttura e significato ai dati grezzi. Sono dati che descrivono altri dati, fornendo informazioni sulle caratteristiche, le proprietà o le relazioni dei dati stessi. I metadati sono essenziali per la gestione, l'organizzazione, l'integrazione, la migrazione e l'uso dei dati. Possono essere utilizzati per migliorare l'interpretazione e la comprensione dei dati, facilitarne la ricerca, la selezione e l'accesso controllato, e per garantirne la qualità, l'affidabilità e la riproducibilità nel tempo. Da notare, inoltre, come questi metadati si prestino ad essere condivisi in un framework "OpenData" che consente di creare un ecosistema in cui varie aziende generano valore condiviso. Questo perché il metadato perde alcune delle caratteristiche di origine della sorgente e diventa neutro, preservando quindi elementi di privacy e di confidenzialità, ma al contempo acquisisce altre caratteristiche necessarie per rendere i dati F.A.I.R, ossia Findable, Accessible, Interoperable, Reusable e per fornire una semantica comune a diverse sorgenti di dati.

L'IA è uno strumento efficace sia per generare metadati sia per metterli a valore. Un esempio rilevante in ambito IA sono le etichette (o label) associate a un dataset. Le etichette sono informazioni aggiuntive associate ai dati di un dataset per associare il contenuto ad una specifica classe in una tassonomia.

Nel contesto dell'apprendimento automatico, ad esempio, in un problema di classificazione di immagini, le etichette potrebbero indicare le categorie di oggetti presenti nelle immagini, come "cane", "gatto", "automobile", ecc. Queste etichette fungono da metadati che descrivono la natura dei dati di addestramento e forniscono informazioni strutturate aggiuntive che specificano e descrivono i dati grezzi contenuti nel dataset. Quindi, l'IA sfrutta i metadati nell'apprendimento automatico, ma l'IA può anche essere utilizzata per generare metadati in diversi modi. Ecco alcuni esempi.

- **Estrazione di caratteristiche**:

L'IA può essere addestrata per estrarre automaticamente caratteristiche significative dalle immagini o dai dati provenienti da sensori. Ad esempio, un modello di apprendimento profondo può essere addestrato per riconoscere e contare forme, colori e pattern specifici in un'immagine o per identificare andamenti specifici costanti, crescenti, decrescenti, intermittenti, ecc. Queste

caratteristiche estratte possono quindi essere utilizzate come metadati strutturati per descrivere l'informazione grezza.

- **Categorizzazione automatica**:

L'IA può essere utilizzata per categorizzare automaticamente le immagini o i dati dei sensori in base a determinati criteri. Ad esempio, categorizzare immagini in base al contenuto, come ad esempio paesaggi, ritratti e nature morte, o per categorizzare sequenze di dati IoT come sequenze normali o sequenze che presentano anomalie o guasti o, ancora, per elaborare dati relativi alla relazione con i clienti per classificarli in diverse classi in base al livello di fidelizzazione o al rischio di churn.

- **Generazione di descrizioni, schemi o riassunti**:

L'IA può essere utilizzata per generare automaticamente contenuti descrittivi dell'informazione grezza proveniente da immagini o sensori. Ad esempio, un modello di generazione del linguaggio naturale può essere addestrato per creare descrizioni testuali di immagini, includendo informazioni strutturate come luogo, data, condizioni meteorologiche, oggetti rilevati e altre caratteristiche pertinenti.

- **Predizione di metadati mancanti**:

L'IA può essere utilizzata per predire metadati mancanti o incompleti basandosi su modelli di apprendimento automatico addestrati su dati reali esistenti. Ad esempio, se alcuni metadati sono incompleti, un modello di predizione può essere utilizzato per stimare tali metadati mancanti in base alle informazioni disponibili. Questi metadati predetti possono essere utilizzati per completare e arricchire l'informazione grezza.

- **Qualità dei dati:**

le misure continue di caratteristiche di qualità dei dati come accuratezza, consistenza, completezza, tempestività, ecc. sono esse stesse metadati. L'IA può essere utilizzata per monitorare in modo continuo la qualità dei dati nel tempo. Ad esempio, possono essere sviluppati modelli di IA per rilevare cambiamenti nella qualità dei dati, come la presenza di dati invalidi o anomali, e per intraprendere azioni correttive.

In sintesi, l'IA può essere utilizzata per generare metadati strutturati che specificano e descrivono l'informazione grezza proveniente da immagini,

tracce audio o in generale da sensori, migliorando la comprensione e l'utilizzo di tali dati in diversi contesti, la gestione dei dati e altro ancora.

I metadati però sono anche importanti perché possono essere utilizzati per spiegare come un modello di IA è stato addestrato, come è stato valutato e come funziona: ad esempio, le IA "spiegabili" possono fornire metadati sull'origine e sul peso specifico che hanno avuto certe tipologie dati nella previsione o nel suggerimento generati.

Queste informazioni inoltre possono consentire agli utilizzatori di valutare la fiducia e l'affidabilità dei dati condivisi e trovati. A questo proposito i metadati, in unione con tecnologie di blockchain permettono di garantire la ownership ed anche di assicurare l'accountability, entrambi elementi essenziali per un contesto di business. In questo contesto, la tecnologia blockchain, può offrire una piattaforma decentralizzata e immutabile per la registrazione dei metadati. Inoltre, la blockchain può fornire meccanismi di consenso distribuito che consentono una governance condivisa e decentralizzata dei metadati stessi.

1.1.7. Dati sintetici

L'Intelligenza artificiale (IA) sta rivoluzionando tutti gli aspetti della nostra vita. Purtroppo, però, moltissimi dei progetti di IA che vengono avviati non riesce a decollare. Questo avviene perché i progetti di IA, per poter essere avviati, hanno bisogno di grandi quantità di dati. Le organizzazioni devono avere accesso a tali dati e assicurarsi che siano significativi, sicuri e utilizzabili. Si tratta di un processo costoso in termini di denaro e di tempo.

La tecnologia dei dati sintetici si sta imponendo come elemento chiave per implementare con successo progetti di Intelligenza artificiale e *data analytics*. I dati sintetici non sono raccolti attraverso tradizionali metodi empirici ma vengono generati algoritmicamente. In quanto tali, non possono essere collegati ad alcuna persona del mondo reale; inoltre, grazie a determinate tecniche di IA, i dati sintetici possono comportarsi come quelli reali. Di conseguenza, il vantaggio principale di questa tecnologia consiste nel coniugare privacy, innovazione e velocità di sviluppo.

I dati sintetici altamente realistici vengono costruiti attraverso tecniche di Intelligenza artificiale generativa. In particolare, i metodi di IA generativa hanno

il compito di dedurre i pattern statistici di un dataset reale per poi replicarli in un dataset sintetico. Se l'inferenza dell'IA avviene con successo, i nuovi campioni di dati avranno lo stesso comportamento dei dati reali. Ciò significa che i dati sintetici ottenuti possono essere utilizzati al posto di quelli reali per ogni tipo di applicazione, tra cui: business intelligence; analisi avanzate; software testing; demo di prodotto; sviluppo di modelli di IA per la previsione, la personalizzazione, la profilazione e altro ancora.

I dati sintetici consentono dunque alle organizzazioni di valorizzare i propri dati. In particolare, consentono di scambiare e analizzare i dati in modo sicuro e libero, e di sopperire alle carenze di dati attraverso la *data augmentation*. I vantaggi principali sono:

- Riduzione di tempi e costi: i dati sintetici non sono soggetti agli stessi protocolli e trattamenti dei dati reali. Ciò riduce le risorse monetarie, temporali e umane nei progetti di IA.
- Dati completi e corretti: i dati sintetici possono essere utilizzati anche nel caso in cui non siano disponibili dati reali sufficienti. Ad esempio, nello studio delle malattie rare, i dati sintetici possono aumentare artificialmente il numero di cartelle cliniche dei pazienti, consentendo di migliorare gli strumenti di prognosi e di diagnosi messi a disposizione dall'IA. Possono anche essere utilizzati per eliminare i bias, aumentando artificialmente la significatività di gruppi sottorappresentati.
- Protezione della privacy dei dati: i dati sintetici conciliano l'utilità dei dati con la protezione della privacy.
- Maggiore mobilità e disponibilità dei dati: i dati sintetici possono essere condivisi liberamente all'interno di un'organizzazione e tra più organizzazioni diverse. Ciò consente per esempio alle organizzazioni sanitarie di affidarsi a consulenze esterne per l'analisi dei dati.
- Flessibilità e centralità dei dati: i dati sintetici possono essere costruiti nella quantità desiderata e con le proprietà desiderate.

È interessante notare come la Generative AI sia anche basata su questa tipologia di dati, che a loro volta sono costruiti da enormi masse di dati "reali", come illustrato in figura:

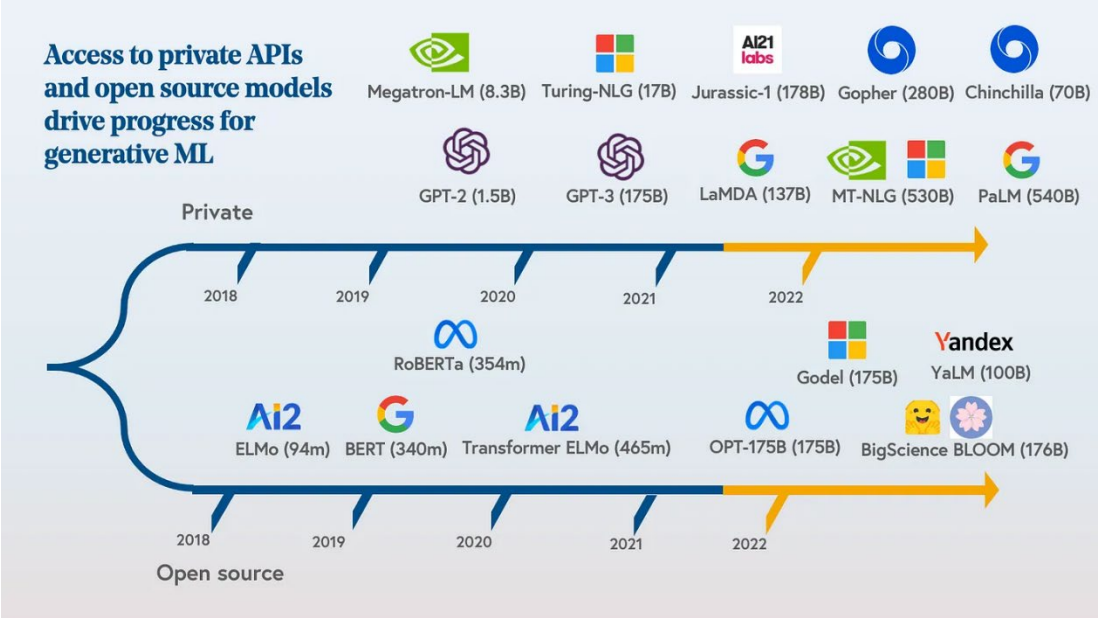


Figura 7. Evoluzione della Generative AI sia sul versante Open Source sia su quello privato (che tuttavia spesso rende disponibile l'accesso alla Generative AI sia tramite interfacce Web sia tramite API.

La figura[5] mostra una varietà di "strumenti" resi disponibili attraverso API – Application Programming Interface- che sono basati su dati sintetici creati a partire da enormi masse di dati reali, generati da analisi di testi, immagini, video, suoni, e dati 3D (ad esempio generati da LIDAR posti su veicoli). In questa figura sono riportati, a fianco di ciascun strumento, la quantità di dati generati (sintetici) che servono allo strumento per "generare" le risposte. Si noti il progressivo incremento dimensionale di queste basi di dati da qualche decina di milioni (ELMo – 94 milioni) a centinaia di miliardi (PaLM – 540 miliardi).

Per le aziende i dati sintetici rivestono un interesse come elemento di partenza, ad esempio per addestrare sistemi di IA, e, potenzialmente, anche in termini di offerta (dati sintetici generati da una azienda potrebbero essere di interesse per un'altra azienda operante in un settore simile. È ovvio che una azienda non disponga di una quantità di dati paragonabile a quelli utilizzati dai "transformer" evidenziati in figura ma i dati aziendali, opportunamente trattati, possono essere associati a quelli dei transformer per creare particolarizzazioni in uno specifico settore di utilizzo.

[5] https://www.bvp.com/atlas/roadmap-the-rise-of-synthetic-media

Per poter costruire algoritmi che apprendono correttamente ed efficacemente dai dati è necessario che questi siano disponibili e di qualità. Sono molteplici gli impatti che si possono avere quando si riscontrano carenze in uno e/o l'altra condizione in cui i dati possono trovarsi. Alcuni degli impatti possono essere affrontati con tecniche basate sulla loro generazione sintetica, ovvero creando dati artificiali che imitano in tutto e per tutto le caratteristiche di quelli reali, ma senza esporli.

Focus: Synthetic Data Generation Models

Diversi modelli di Synthetic Data Generation (SDG) permettono di generare dati sintetici o ampliare quelli esistenti, con una sfida principale: valutarne l'output. A questo proposito si utilizzano metriche, di tipo ristretto o ampio, per assicurare la qualità del dato prodotto e confrontare i vari SDG.

Le metriche ristrette esaminano proprietà specifiche dei dati, come somiglianza o diversità, mentre quelle ampie offrono una valutazione olistica del SDG, e cercano di prevedere buone metriche ristrette anche senza conoscere a priori i casi d'uso. Esistono anche metriche focalizzate sulla bontà del dataset e altre focalizzate sul modello di generazione, con queste ultime spesso preferite per la valutazione dei SDG data la natura stocastica dei modelli generativi. L

a valutazione può essere umana, che per quanto diretta è costosa e non sempre applicabile, o basata sul confronto statistico tra dati reali e sintetici, utilizzando vari tipi di statistiche. Nonostante esistano diversi approcci e metriche di valutazione, stabilire misure di qualità che catturino tutti gli aspetti rilevanti è complesso, soprattutto in domini delicati come quello medico. La generazione di dati sintetici presenta sfide come la copertura di casi limite e l'addestramento su dataset potenzialmente bias.

Nonostante le imperfezioni e le sfide del metodo SDG, la comunità di ricercatori è generalmente ottimista sul suo impatto e rilevanza crescenti grazie all'evoluzione di modelli, metriche e tecnologie.

1.2. Trattamento dei dati

1.2.1. Cloud

Recenti studi sullo sviluppo di soluzioni basate sulla IA hanno dimostrato l'importanza della scalabilità per questa tecnologia in termini di benefici per la società e per le aziende.

Il paradigma Cloud rappresenta il metodo migliore per mettere a disposizione tecnologie, prodotti e soluzioni su cui ospitare applicazioni basate sull'IA, senza trascurare la sicurezza, il controllo e la trasparenza, nella consapevolezza che la mancanza di qualità dei dati e la conformità alle regole vigenti possono essere un problema e una sorgente di costi.

Esistono attualmente molte tecnologie abilitanti il Cloud computing, che si posizionano sui vari livelli dello *stack* tecnologico, ad esempio:

- l'infrastruttura – ovvero la base della computazione in termini di risorse, storage, network, sicurezza, distribuzione dei data center e relativi servizi; la piattaforma – costruita sullo strato infrastrutturale, che mette a disposizione tutti i tool e gli ambienti di sviluppo;
- le applicazioni e i modelli – ovvero sistemi pre-pronti utilizzabili per arricchire e infondere di IA le applicazioni.

A contorno di questo stack applicativo, distribuito in varie modalità e con diverse tecnologie da vari Cloud Service Provider, vi è un elenco di *tool* per lo sviluppo, ottimizzazione, distribuzione, controllo e conformità per mettere l'IA al servizio delle applicazioni in modo sicuro e senza sorprese in termini di costi nascosti o di rischi.

I benefici di un approccio Cloud per l'IA, come detto, sono molteplici ma riguardano soprattutto il miglioramento della produttività con uno sviluppo e una distribuzione dei modelli più veloce, più sicuro e certificato (secondo le regole imposte dallo specifico cliente, dall'industria o dallo Stato di riferimento).

Tra i vari prodotti Cloud disponibili sul mercato per l'IA, spiccano le soluzioni per supportare il cosiddetto "AI journey", il viaggio verso il raggiungimento di un vantaggio competitivo tramite l'adozione di IA, ad esempio, nei processi aziendali: queste soluzioni comprendono **sistemi di automazione**, **ottimizzazione proattiva dell'IT**, **lavoro digitale**, **cybersecurity**, **gestione del ciclo di vita dei modelli di machine learning** e molto altro. Nei prossimi paragrafi è riportata una lista di aree applicative nell'ambito IA coperte da tipologie di servizi Cloud.

- Piattaforme di sviluppo agile: abilitano gli sviluppatori e i data scientist a costruire e scalare facilmente modelli di machine learning attraverso ambienti on-demand. Esempi: AWS Sagemaker, IBM Watson Studio, Google Vertex AI.

- Servizi di conversazione: creazione di bot per velocizzare l'interazione con gli utenti e i clienti. Esempi: Azure Bot, IBM Watson Assistant, Amazon Lex, Google DiagFlow.
- Servizi di ricerca/analisi/scoperta: applicazione del natural language processing per recuperare insight sui dati in modo veloce ed ottimizzato. Esempi: IBM Watson Discovery, NeuralSeek, Amazon Comprehend.
- Computer vision: analisi di immagini e video. Esempi: Amazon Rekognition, IBM Maximo, Azure Video Indexer, Google Vision AI.

Oltre ai servizi relativi prettamente all'IA, esistono molte altre tecnologie abilitanti che possono essere utilizzate in modalità Cloud (database, object storage, servizi di computazione serverless, etc…).

Infine, è utile ricordare che **oltre ai Cloud Service Provider pubblici**, **il paradigma Cloud per l'IA può creare grandi vantaggi applicando un approccio ibrido**, in cui un ambiente Cloud o Multi-Cloud pubblico viene affiancato ed integrato con un ambiente *on-premises*.

Gli use case e i vantaggi di questo modello sono molteplici: alcuni esempi sono riportati di seguito.

- Utilizzo dei servizi Cloud pubblici sfruttando la loro scalabilità virtualmente "illimitata": creazione, training continuo e distribuzione su larga scala e in varie regioni del globo di modelli di IA.
- Utilizzo di ambienti Cloud pubblici dedicati, sfruttando la scalabilità tipica degli ambienti pubblici e la sicurezza degli ambienti privati, es. server fisici dedicati in modalità Cloud indicati per carichi di lavoro general-purpose e per HPC, ad esempio indicati per la gestione di grandi quantità di dati durante il training dei modelli IA.
- Accesso ad elevata potenza computazionale on-premises con tecnologie specifiche (ad esempio Mainframe o LinuxONE) e i processori creati appositamente per l'IA: i modelli di deep learning possono richiedere enormi potenze di calcolo, tali per cui anche CPU e GPU possono risultare inadeguate. Le AIU – Artificial Intelligence Unit – sono processori appositamente sviluppati per velocizzare i processi di training.
- *Retention* dei dati sensibili su ambienti privati on-premises o Cloud pubblici Privati (ad esempio gli ambienti di Confidential Computing come IBM Cloud Hyper Protect): specifici modelli di machine learning che

gestiscono dati regolamentati e particolarmente sensibili possono essere eseguiti privatamente su infrastruttura on-premises o Cloud pubblica Privata, sfruttando gli ambienti di sviluppo su Cloud pubblici per il training (se eseguito senza dati regolamentati).

L'integrazione degli ambienti in modalità Cloud ibrido è possibile condiverse modalità e tecnologie (ad esempio AWS Outposts, Google Anthos, Azure Stack, e in particolare IBM Cloud Satellite per quanto riguarda gli ambienti ibridi e Multi-Cloud), in modo da creare un ambiente unico in cui il flusso applicativo possa usufruire della miglior opzione in ogni momento, come ad esempio ambienti dedicati mentre si maneggiano dati confidenziali, o ambienti pubblici, scalabili e agili quando non vi sono particolari restrizioni.

1.2.2. Security

L'IA presenta sfide e rischi per la sicurezza e la protezione dei dati (personali e non) che vengono in contatto con questa tecnologia, sia per il suo funzionamento normale sia per la fase di apprendimento e costruzione delle IA. **In questo capitolo verranno trattati i concetti generali di sicurezza del dato in ambienti informatici, e come tali concetti sono stati declinati dalla comunità nei sistemi di Intelligenza artificiale.**

Per sicurezza dei dati in sistemi e piattaforme informatiche, e nel nostro caso nelle piattaforme di IA, si intende l'insieme delle misure tecniche e organizzative volte a proteggere i dati da possibili violazioni, perdite, alterazioni o accessi non autorizzati. Tali dati, soprattutto negli scenari che coinvolgono l'IA, rappresentano per le organizzazione degli asset preziosi ("crown jewels" o "gioielli della corona" in gergo tecnico), in quanto generati, raccolti e classificati spesso dalle organizzazioni stesse e in quanto fondamentali per l'apprendimento e il funzionamento delle IA.

La sicurezza del dato, in informatica, si basa su tre principi fondamentali:

- **Confidenzialità**: significa garantire che i dati e le risorse siano accessibili solo a chi ne ha il diritto e il consenso;
- **Integrità**: significa garantire che i dati e le risorse non siano modificati o danneggiati da agenti esterni o interni;

- **Disponibilità**: significa garantire che i dati e le risorse siano accessibili e fruibili in ogni momento da chi ne ha il diritto e il bisogno.

L'IA, peraltro, può basarsi su dati di natura personale o sensibile, che possono riguardare la salute, le preferenze, le opinioni, il comportamento o l'identità degli individui. Pensiamo ad esempio ad una IA, utilizzata in una banca, per aiutare il personale nella valutazione economiche delle persone richiedenti di un mutuo, oppure una IA utilizzata in ambito sanitario per la valutazione automatica di cartelle cliniche. Queste IA prese utilizzano dati critici sia in fase di apprendimento, sia in fase di funzionamento normale. **In questi casi di esempio, la messa in sicurezza diventa ancora più critica trattandosi di dati coinvolti anche da legislazioni dedicate europee e nazionali.**

Più genericamente, **nei sistemi di IA la gestione dei dati presenta delle sfide specifiche per la sicurezza di essi, che richiedono una maggiore attenzione e vigilanza da parte dei responsabili della gestione e da parte dei proprietari del dato.**

Tra queste sfide possiamo citare:

- **Mantenimento dell'integrità dei dati** utilizzati per addestrare e testare i sistemi di IA, che se alterati possono influenzare la loro accuratezza, affidabilità e imparzialità;
- **Mitigazione e gestione dei rischi di violazione**, manipolazione o perdita dei dati a causa di attacchi informatici o errori umani o tecnici;
- **la messa in sicurezza del ciclo di vita di una IA**, il quale risulta molto complesso a causa della complessità stessa della tecnologia.

Queste sfide assumono particolare significato nel sistema Italia, dove nel panorama Cybersecurity sono stati osservati dati di tendenza peggiorativi per quanto riguarda gli attacchi informatici alle realtà del nostro paese. Secondo il report CLUSIT 2023 infatti:

- Nel 2022 in Italia è andato a segno il 7,6% degli attacchi globali (contro il 3,4% del 2021);
- In numero assoluto sono stati 188 gli attacchi verso il nostro Paese, dato che segna un incremento del 169% rispetto al 2021[8].

[8] https://clusit.it/rapporto-clusit/

Per affrontare queste sfide in un panorama così complesso è necessario adottare un **approccio alla Security specifico per l'Intelligenza artificiale**.

Inoltre, è fondamentale rafforzare le capacità di difesa e di reazione alle minacce cyber che possono compromettere l'integrità, la disponibilità e la confidenzialità dei dati coinvolti nei sistemi di IA. A tal fine, è raccomandato:

- effettuare una **valutazione approfondita delle minacce** (Threat Modeling) per identificare preventivamente i potenziali incidenti di sicurezza in maniera da indirizzarli adeguatamente con dei controlli di sicurezza dedicati;
- adottare **misure tecniche e organizzative adeguate** per prevenire e contrastare gli attacchi informatici, come la cifratura dei dati, la segmentazione delle reti, l'autenticazione multifattoriale, il backup dei dati, la gestione degli accessi e degli incidenti;
- seguire le **best practices e gli standard internazionali di cybersecurity**, come quelli proposti dall'European Union Agency for Cybersecurity (ENISA), dal National Institute of Standards and Technology (NIST) o dalla Cybersecurity and Infrastructure Security Agency (CISA) degli Stati Uniti;
- **formare e sensibilizzare il personale** e gli utenti sui rischi e le responsabilità legati all'utilizzo dell'IA e sulle misure di prevenzione e protezione da adottare;
- **monitorare e valutare costantemente le performance e gli impatti dei sistemi di IA**, con particolare attenzione alla gestione degli errori, delle anomalie e delle vulnerabilità.

Un focus sulle sfide della messa in sicurezza delle intelligenze artificiali è stato messo nel documento prodotto dall'ENISA (European Union Agency for Cybersecurity) chiamato "Artificial Intelligence Cybersecurity Challenges"[10]. Tale relazione presenta la mappatura del panorama delle minacce nel settore IA creata dall'ENISA, realizzata con il supporto di un gruppo di lavoro dedicato sulla cybersecurity nell'Intelligenza artificiale.

Il report di ENISA non solo pone le basi per le prossime iniziative politiche e le linee guida tecniche in materia di cybersecurity, ma sottolinea anche le sfide rilevanti che devono essere affrontate per l'utilizzo sicuro delle intelligenze

[10] https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

artificiali. Il documento definisce l'ecosistema dell'IA nel contesto della cybersecurity seguendo un **approccio basato sul ciclo di vita**, identifica gli **asset dell'ecosistema di IA**, mappa il **panorama delle minacce all'IA** mediante una tassonomia dettagliata, **classifica le minacce per i diversi asset** e nelle diverse fasi del ciclo di vita dell'IA, ed elenca i **possibili attori delle minacce.**

1.2.3. Quantum

Il computer quantistico, tecnologia teorizzata agli inizi degli anni 80 e ancora in fase di sviluppo, rappresenta l'ultima evoluzione del paradigma computazionale.

Diversamente rispetto alla computazione classica, dove ogni calcolo – dalle operazioni più semplici fino ai più complessi sistemi di machine learning – si basa sulla manipolazione di stringhe binarie (composte da serie di 0 e 1), un computer quantistico presenta un metodo diverso di concepire l'unità fondamentale del calcolo. Il qubit, ovvero l'analogo quantistico del bit, è il sistema alla base del computer quantistico: è regolato dalle leggi della meccanica quantistica (ad esempio la sovrapposizione, l'entanglement e l'interferenza), e può sfruttarle per ampliare la potenza computazionale fino a raggiungere, al limite, uno speed-up esponenziale per alcune classi di problemi rispetto ad un approccio classico. Su approfondimenti sul quantum computing in generale rimandiamo ai White Paper Anitec-Assinform: "*Il Quantum Computing a supporto della trasformazione digitale italiana*"[11] e "*Tecnologie Quantistiche per la Sicurezza delle Comunicazioni Digitali*"[12]

Nel campo della IA, i ricercatori sono molto interessati a capire come sfruttare la potenza di calcolo dei computer quantistici, con l'obiettivo di capire se un approccio quantistico potrò dare un effettivo vantaggio in particolare durante la fase di training dei modelli. Per questo motivo, l'attenzione del settore sulla

[11] Disponibile online: https://www.anitec-assinform.it/pubblicazioni/policy-paper/quantum-computing.kl

[12] Disponibile online: https://www.anitec-assinform.it/pubblicazioni/policy-paper/quantum-secure-communications.kl

ricerca di ambiti di applicazione pratica e vantaggiosa del *quantum computing* nell'IA e nel *machine learning* è molto alta.

Sono già stati identificati alcuni ambiti molto promettenti relativi al quantum computing per l'IA, ad esempio l'ottimizzazione del training dei modelli, il riconoscimento di pattern (ovvero la scoperta di strutture difficili da identificare all'interno di dataset per aumentare l'accuratezza della classificazione), l'intercettazione delle frodi, lo studio e la previsione di comportamenti chimico/fisici (ad esempio sulla scoperta e sulla sintetizzazione di medicinali), e molti altri.

Riportiamo una lista di use case del quantum computing per l'IA.

- **Smart manufacturing**: le iniziative di trasformazione digitale tramite IA degli ambienti produttivi di fabbrica stanno raggiungendo il loro limite superiore. L'IA viene utilizzata ad esempio per distinguere manufatti con difetti di produzione da manufatti senza difetti; per andare oltre gli attuali limiti dell'IA classica, un approccio quantistici riesce a migliorare l'accuratezza e velocizzare il training, e a raggiungere risultati migliori in termini di errore rispettivamente alla quantità di dati in ingresso.
- **Diagnosi mediche**: la classificazione delle immagini è molto importante nell'ambito delle analisi mediche di imaging; sistemi basati su IA classica stanno attualmente aiutando i medici ad analizzare più velocemente ed accuratamente le immagini, mentre un futuro approccio quantistico come il quantum support vector machine learning (QSVML) potrà migliorare l'accuratezza della classificazione ed essere in grado di analizzare singole cellule, aprendo la via alla medicina di precisione.
- **Sviluppo di medicinali tramite lo studio del ripiegamento delle proteine**: la produzione di anticorpi, insulina e molti vaccini si basa attualmente su complicati modelli tridimensionali delle molecole; l'approccio classico alla computazione sta velocemente raggiungendo i suoi limiti, in quanto le molecole oggetto di studio stanno diventando sempre più complesse per ottenere risultati sempre migliori. Si dimostra necessario quindi compiere delle approssimazioni, in quanto le configurazioni molecolari delle proteine possono raggiungere un numero di 10^{47}, rendendo i modelli di machine learning molto difficili da gestire. Un approccio quantistico potrà migliorare drasticamente la potenza di calcolo per studiare e predire il ripiegamento delle proteine, utilizzando oltretutto dati di training in quantità limitata.

- **Gestione delle interruzioni di forniture**: la recente pandemia ha dimostrato come una interruzione improvvisa delle forniture possa causare uno shock globale. Un approccio quantistico per simulare gli impatti e la logistica in caso di interruzione globale può migliorare il processo decisionale migliorando il recupero, abbassando i costi e riducendo i disservizi. Per di più, il miglioramento dei processi di IA tramite il quantum machine learning può aiutare a perfezionare la classificazione degli eventi e la predizione di future interruzioni.

È interessante avere una proiezione temporale di quando un approccio quantistico all'IA diventerà fattuale e vantaggioso. Sono disponibili diverse *roadmap* di sviluppo delle tecnologie quantistiche; Alcune stime[13] propongono il 2025 come target per raggiungere i primi prototipi di applicazioni quantum machine learning vantaggiose, andando di pari passo con lo sviluppo dell'hardware (in termini di numero di qubit, qualità e velocità dei processori), delle componenti software di base (error mitigation/suppression/correction) e degli algoritmi (ottimizzazione dei circuiti, orchestrazione della computazione classica e quantistica, approccio serverless e multi-cloud).

Come fare per iniziare ad esplorare il mondo del quantum computing applicato all'IA? Un metodo può essere esplorare i framework di sviluppo open-source che presentano specifiche aree, librerie ed applicazioni rivolte al machine learning, come ad esempio Qiskit Machine Learning[14]: sono già presenti in rete molti tutorial relativi alle reti neurali quantistiche, alle reti neurali convoluzionali quantistiche, ai classificatori e regressori quantistici, e su come effettuare il training, salvataggio e caricamento dei modelli.

1.2.4. Profili di privacy e regolazione

È facilmente intuibile la vastità degli scenari privacy che si aprono sul tema dell'Intelligenza artificiale, dando origine ad infiniti interrogativi e ad un intenso dibattito sotto il profilo etico, tecnico, sociale e – ovviamente – di tutela dei dati personali. Ed è proprio su quest'ultimo aspetto che si concentrerà il focus di questo capitolo.

[13] https://www.ibm.com/quantum/roadmap
[14] https://qiskit.org/documentation/machine-learning/

Per capire lo stato attuale della normativa sul tema è utile ripercorrere rapidamente l'evoluzione legislativa che fin dai primi tentativi di applicazione delle tecnologie IA ai trattamenti di dati personali, ha visto impegnati le diverse Autorità, Garante Privacy e Parlamento europeo *in primis*.

I principi cardine per la costruzione di una normativa sull'AI: origini e premesse

Sin dalle prime fasi dello sviluppo della tecnologia dell'AI, l'Autorità Garante ha intuito i rischi connessi al suo impiego e l'impatto che l'utilizzo a tappeto di dati e meta-dati avrebbe avuto. Già nell'**epoca pre-GDPR** il Garante si era pronunciato contro i trattamenti basati sull'analisi comportamentale degli utenti utilizzata da alcuni siti commerciali, aveva bocciato il sistema di rating reputazionale fondato sul *data scraping* in Rete, così come i sistemi di lettura biometrici installati sui totem pubblicitari.

Posizioni queste che– con l'entrata in vigore del **GDPR** – hanno trovato piena applicazione nei principi cardine del Regolamento europeo a partire dall'**Articolo 22** che, ponendo l'accento sul trattamento automatizzato dei dati personali, ribadisce il diritto dell'Interessato di non essere sottoposto a una decisione basata esclusivamente sul trattamento automatizzato dei propri dati, profilazione in primis, descritta nell'**Art. 4** del GDPR.

Articoli a cui fanno seguito i successivi - di fondamentale importanza per chi progetta sistemi di IA - quali l'**Art. 24** Responsabilità del titolare del trattamento) che introduce il principio cardine di ***accountability*** secondo cui "*tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*" e *il successivo* ***Articolo 25***. Quest'ultimo portavoce dei principi di ***privacy by design e by default*** secondo cui la protezione dei dati dovrebbe essere parte integrante di ogni processo industriale e tecnologico, che implichi la produzione di beni e servizi che - in una qualunque fase - comportino il trattamento di dati personali, segna di fatto un cambio di prospettiva epocale. Con questo principio, a ben vedere, la normativa, solitamente astratta e

disgiunta dalla tecnologia e dal mercato, viene catapultata sul terreno attuale e del futuro, in continua evoluzione, divenendo lo strumento più prezioso per cogliere le opportunità offerte dalla scienza e schivare – o perlomeno limitare – le insidie del progresso ai danni della libertà e dei diritti fondamentali-

Il crescente impegno normativo per disciplinare l'AI, dal GDPR al caso ChatGPT

Dopo la pubblicazione del GDPR, l'urgenza europea di muoversi rapidamente verso regole sull'IA armonizzate e condivise è stata sottolineata anche dai successivi interventi della Commissione. Ricordiamo l'**intervento del 2017** con cui il Consiglio europeo ha invitato a dimostrare la *"consapevolezza dell'urgenza di far fronte alle tendenze emergenti*", comprese "*questioni quali l'Intelligenza artificiale …, garantendo nel contempo un elevato livello di protezione dei dati, diritti digitali e norme etiche*".

Così come ricordiamo le **conclusioni del 2019** sul piano coordinato sullo sviluppo e l'utilizzo dell'Intelligenza artificiale "Made in Europe", in cui *"il Consiglio ha inoltre posto l'accento sull'importanza di garantire il pieno rispetto dei diritti dei cittadini europei e ha esortato a rivedere la normativa pertinente in vigore con l'obiettivo di garantire che essa sia idonea allo scopo alla luce delle nuove opportunità e sfide poste dall'Intelligenza artificiale. Il Consiglio europeo ha inoltre invitato a definire in maniera chiara le applicazioni di IA che dovrebbero essere considerate ad alto rischio"* seguite dalle **conclusioni del 21 ottobre 2020** in cui *"si esortava inoltre ad affrontare l'opacità, la complessità, la faziosità, un certo grado di imprevedibilità e un comportamento parzialmente autonomo di taluni sistemi di IA, onde garantirne la compatibilità con i diritti fondamentali e agevolare l'applicazione delle norme giuridiche*".

Numerose sono state inoltre le attività intraprese dal Parlamento europeo sul fronte AI. Rammentiamo le risoluzioni nell'**ottobre 2020**, riguardanti anche etica, responsabilità e diritti d'autore, seguite l'anno successivo da altre risoluzioni in ambito penale.

Un impegno giurisprudenziale sempre più attivo, rimasto sul piano dei principi **fino al 2021**, anno decisivo che ha segnato una svolta notevole con la presentazione del **Regolamento sull'Intelligenza artificiale**, in

costruzione. Fino ad arrivare al più recente **primo semestre 2023**, in cui - complici anche gli incalzanti fatti di cronaca - si è reso necessario il tempestivo intervento dell'Autorità. Ricordiamo il caso Chat GPT per cui il Garante è intervenuto con un provvedimento con effetto immediato a **fine marzo 2023** dopo aver rilevato "*la mancanza di una informativa agli utenti e a tutti gli interessati i cui dati vengono raccolti da OpenAI, ma soprattutto l'assenza di una base giuridica che giustifichi la raccolta e la conservazione massiccia di dati personali, allo scopo di 'addestrare' gli algoritmi sottesi al funzionamento della piattaforma. Come peraltro testimoniato dalle verifiche effettuate, le informazioni fornite da ChatGPT non sempre corrispondono al dato reale, determinando quindi un trattamento di dati personali inesatto*".

Sospensione superata proprio nei giorni scorsi con la regolarizzazione della propria posizione da parte di OpenAI, che dopo aver ha dimostrato il recepimento di buona parte delle prescrizioni imposte dal Garante, ha ripristinato il servizio, fermo restando l'attività istruttoria in corso.

Lo si può considerare un provvedimento certamente esemplare, che ha rappresentato di fatto un fortissimo segnale per le imprese attive nell'ambito AI, sottolineando l'importanza del rispetto delle norme privacy e della protezione dei dati. Una ragione in più per le imprese del settore, d'ora in avanti più che mai nel mirino dell'Autorità, per prendere consapevolezza dei risvolti giuridici sull'uso e gli effetti di tali soluzioni ed impegnarsi nella ricerca di un equilibrio adeguato tra business e prescrizioni normative.

1.3. Leverage sui dati

1.3.1. Analytics

Oggi gli Analytics sono fondamentali per le aziende, affinché riescano a valorizzare le grandi moli di informazioni originate da diverse sorgenti come dispositivi mobili, sensori IoT (Internet of Things), apparecchiature audio/video, reti, file di log, applicazioni transazionali, web e social media.

Data la varietà di forma e dimensione dei dati, essi vengono identificati come "Big Data", i quali possono essere memorizzati all'interno di database strutturati, non strutturati, storage, data warehouse, Data lake e data lakehouse.

Indipendentemente dalla tecnologia utilizzata per memorizzare i dati, l'obiettivo è quello di creare un sistema di archiviazione progettato per raccogliere, organizzare e gestire grandi quantità di informazioni provenienti da diverse fonti, sia strutturati che non strutturati. Memorizzare tutte queste informazioni ha lo scopo di fornire un'importante base dati per la analisi statistiche. Esistono diverse modalità con la quale estrarre conoscenza:

- Analisi descrittiva
- Analisi diagnostica
- Analisi predittiva
- Analisi prescrittiva

Ogni campo di analisi risolve uno specifico problema di business, ad esempio l'analisi descrittiva permette di comprendere in modo più semplice i dati attraverso la fruizione di grafici di vario genere.

L'analisi descrittiva è anche il tipo di analisi meno complesso da attuare mentre, come si evince nel grafico sottostante, al variare dell'analisi aumenta anche la difficoltà. Difficoltà e valore sono direttamente proporzionali: all'aumentare di uno aumenta anche il secondo.

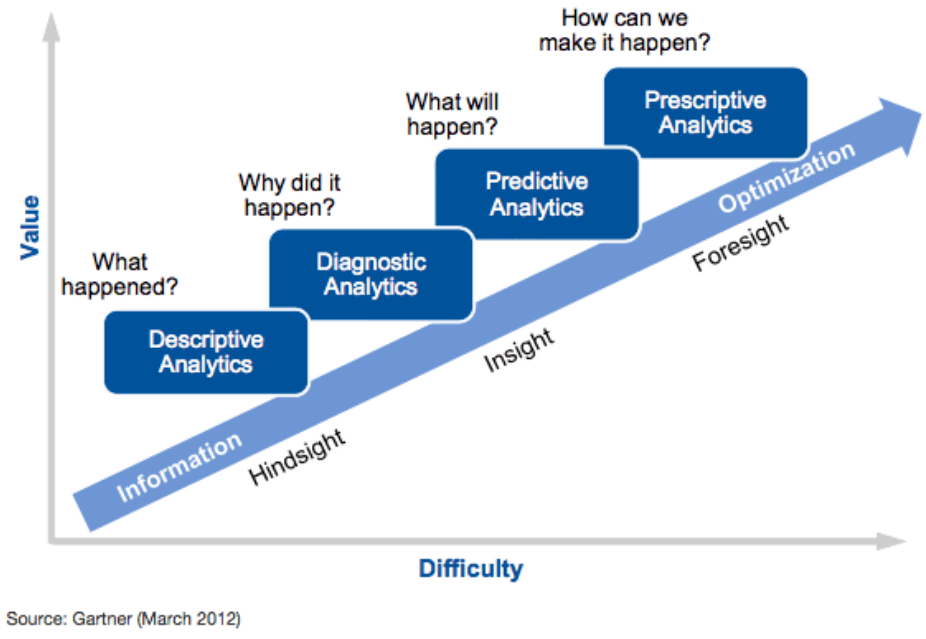


Figura. 8. Analytics, difficoltà e valore. Fonte: Gartner

L'analisi descrittiva si concentra dunque sull'esplorazione e sulla descrizione dei dati esistenti. Questo approccio mira a fornire una panoramica completa e oggettiva dei dati collezionati. L'analisi descrittiva utilizza strumenti e tecniche statistiche per riepilogare e visualizzare i dati, ad esempio mediante grafici, tabelle e KPI statistici (moda, mediana, media, varianza, ecc.).

L'obiettivo principale dell'analisi descrittiva è quindi rispondere a domande come **"Quali sono le caratteristiche dei dati?".**

L'analisi diagnostica si focalizza invece **sull'individuazione delle cause o dei fattori che hanno condotto a specifici risultati o comportamenti dei dati**. Questo tipo di analisi mira a comprendere le connessioni causali tra le diverse variabili, offrendo spiegazioni sul motivo per cui un evento si è verificato. Per condurre un'analisi diagnostica, vengono impiegati modelli, algoritmi e tecniche avanzate per identificare gli elementi critici che influenzano un fenomeno specifico, come ad esempio l'analisi della correlazione tra la variabile obiettivo e i predittori. Mediante l'analisi diagnostica è possibile rispondere a domande chiave come "Quali sono i principali fattori che contribuiscono a un determinato risultato?".

La terza tipologia di analisi è data dalla statistica predittiva, con essa aumenta la knowledge che è possibile estrarre dai dati ma allo stesso tempo anche la complessità per la realizzazione di modelli di questo genere. Vengono utilizzati algoritmi di Machine Learning e Deep Learning. Essi permettono di predire il comportamento di uno specifico fenomeno statistico basandosi sulle precedenti informazioni raccolte che costituiscono lo storico dei dati. L'obiettivo principale dell'analisi predittiva è quindi rispondere a domande come "Questo cliente mi abbandonerà in futuro?" oppure "Quanto sarà la domanda di questo specifico prodotto nel prossimo mese?".

L'ultima, e più complessa analisi statistica che è possibile eseguire su uno specifico dataset è **l'analisi prescrittiva**. l'analisi prescrittiva si concentra sull'anticipazione del futuro e sulla fornitura di raccomandazioni per guidare le decisioni di business. Essa utilizza algoritmi avanzati, modelli predittivi e tecniche di ottimizzazione per determinare le migliori azioni da intraprendere in base a specifici scenari o funzioni obiettivo. Fornisce dunque raccomandazioni concrete e basate sui dati per migliorare le decisioni aziendali, ottimizzare le risorse e massimizzare i risultati desiderati.

L'analisi prescrittiva trova applicazione in diversi settori e ambiti. Ad esempio, nelle operazioni aziendali, può essere utilizzata per **ottimizzare la catena di approvvigionamento** (Supply chain), **identificando i modelli di domanda futuri e suggerendo le azioni più appropriate per minimizzare i costi o massimizzare l'efficienza**. Nel settore finanziario, l'analisi prescrittiva può aiutare a individuare le strategie di investimento ottimali, tenendo conto di variabili come i rischi, le tendenze di mercato e gli obiettivi finanziari specifici. In ambito sanitario, l'analisi prescrittiva può contribuire a migliorare la gestione delle cure e la pianificazione delle risorse, consentendo di identificare i pazienti a rischio o fornendo linee guida personalizzate per i trattamenti.

L'obiettivo principale dell'analisi predittiva è quindi rispondere a domande come "Dati questi vincoli e un obiettivo finale (come la minimizzazione dei costi), come evolveranno le mie variabili?".

Combinando tutte le metodologie, le organizzazioni possono acquisire una comprensione completa dei dati, consentendo loro di prendere decisioni informate e di formulare strategie più efficaci. Indipendentemente dall'approccio utilizzato, è fondamentale adottare un'analisi basata sui dati per guidare le scelte aziendali, migliorare le prestazioni e ottenere un vantaggio competitivo

1.3.2. Digital Twin

Il Digital Twin (Gemello Digitale) è una rappresentazione digitale di un elemento reale (ad esempio prodotto, processo o infrastruttura.

Si compone di tre elementi:

- Il **modello digitale** (ad esempio il modello del motore di un aereo);
- **L'ombra digitale** (Digital Shadow) cioè l'insieme di dati che rappresentano lo stato del suo gemello fisico (physical twin) in quell'istante (ad esempio i valori di pressione, temperatura, consumo del motore ad un certo istante);
- La **storia digitale** (digital Thread) cioè l'insieme di dati raccolti nel tempo (ad esempio i dati relativi ai componenti del motore, alla supply

chain, a chi ha montato i vari pezzi, all'utilizzo del motore, alle operazioni di manutenzione ….

Questi tre componenti, tutti basati sui dati, permettono di utilizzare il Digital Twin per:

- Monitorare il funzionamento dell'elemento reale (physical twin) – ad esempio monitorare il funzionamento del motore
- Interagire con l'elemento reale per dare istruzioni (comandi) – ad esempio richiedere una diminuzione di potenza per prevenire un surriscaldamento
- Simulare (what if) quale potrebbe essere l'effetto sull'elemento reale di una certa situazione - ad esempio valutare se al perdurare di un certo utilizzo potrebbero manifestarsi problemi o se effettuando certi correttivi, come diminuzione di potenza, il problema può essere tamponato
- Interagire con altri digital twin che rappresentano altri elementi del mondo reale (ad esempio interagire con il digital twin dell'altro motore dell'aereo per compensare la diminuzione di potenza

È evidente che a seconda del settore di utilizzo e del tipo di utilizzo, il digital twin possa avere delle sfumature diverse: ad esempio il digital twin che rappresenta un motore è diverso dal digital twin che rappresenta un sistema robotizzato autonomo che cambia nel tempo, così come è diverso dal digital twin che rappresenta una città o da quello che potrebbe rappresentare un sistema biologico, una cellula, un organo, una persona.

Quello che è importante tener presente è che la tecnologia dei digital twin, nata oltre 15 anni fa e largamente usata nell'industria manufatturiera, continua ad evolvere. In particolare, sono stati identificati cinque stadi di evoluzione:

1. Semplice rappresentazione di un elemento fisico (che potrebbe anche non essere ancora stato realizzato). I sistemi CAD (manifattura) e BIM (costruzioni) creano dei modelli digitali. Questi possono essere arricchiti con del software e dei dati in modo da consentire simulazioni dell'elemento fisico prima che questo sia costruito. L'elemento di digital shadow e di digital thread, in questo caso, è generato a partire da dati sintetici, non essendoci l'elemento fisico che può generarli.

2. Affiancamento all'elemento fisico ma in assenza di connessione diretta. I dati che formano la digital shadow sono forniti da un meccanismo esterno. Il Digital Twin viene utilizzato per simulare l'elemento fisico, visualizzare certi suoi aspetti.
3. Affiancamento all'elemento fisico (in genere acquisendo i dati generati da sensori -IoT trasmessi in tempo reale o quasi reale). Questo consente di monitorare l'elemento fisico attraverso il digital twin.
4. Capacità di svolgere alcune funzionalità che complementano quelle svolte dall'elemento fisico. In questo caso (simile alla esecuzione di funzionalità nel cloud) una perdita di connessione tra Digital Twin e Physical Twin porta ad un degrado delle funzionalità offerte.
5. Autonomia del Digital Twin. Questo consente al Digital Twin di effettuare delle attività per conto dell'elemento fisico, ad esempio comunicare con altri digital twin e coordinare delle azioni.

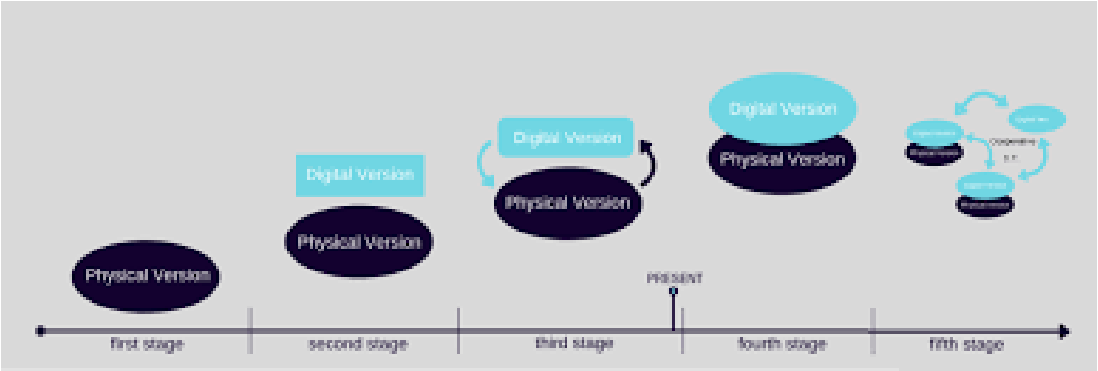


Figura 9. Stati di evoluzione dei Digital Twin, da semplice modello ad agente autonomo.

Quando il Digital Twin opera allo stadio 4 e 5 deve avere una consapevolezza dell'ambiente in cui il suo physical twin opera e degli obiettivi da raggiungere. Per entrambi si fa uso di Intelligenza artificiale "embedded" e questa sta caratterizzando sempre più l'utilizzo e l'evoluzione dei Digital Twin.

Allo stadio 3 è possibile un utilizzo di Intelligenza artificiale "affiancata" al Digital Twin, ad esempio per effettuare simulazioni e what-if analyses.

Dal BIM al Digital Twin

Il Digital Twin nel settore AEC si basa sull'utilizzo di modelli BIM che, uniti ai dati provenienti da diverse fonti come sensori IoT, BMS, azioni registrate da occupanti e manutentori tramite app di field service, diventa un gemello digitale dell'asset aggiornato in tempo reale.

- *Vantaggi*

Un gemello digitale abilita i professionisti del settore a condurre analisi su performance e ottimizzazione del comportamento dell'asset reale, svolgendo dei test di tipo non distruttivo.

L'utilizzo dei Digital Twin ha l'ulteriore vantaggio di raccogliere dati storici sul comportamento di asset di varia natura (immobili, infrastrutture, reti) che, utilizzati da algoritmi di IA, consentirebbero di semplificare, supportare e migliorare la progettazione dei nuovi asset.

- *Digital Twin per l'intero ciclo di vita dell'asset*

Il modo in cui un gemello digitale viene utilizzato dipende dalla fase del ciclo di vita dell'opera che si vuole monitorare e migliorare, ad esempio:

- in fase di costruzione:
    - Il modello BIM strutturale output della fase di progettazione può essere arricchito dai dati provenienti da sensoristica installata sulla struttura in costruzione ai fini del monitoraggio stabilità elementi strutturali
- In fase di operazione:
    - Si possono utilizzare i modelli BIM impiantistici collegati alla sensoristica degli impianti HVAC per il monitoraggio consumi energetici
    - Utilizzo dei modelli BIM architettonici con dati provenienti da sistemi di tracciamento degli occupanti in ingresso/uscita o dall'intero immobile o da una singola zona al fine di controllare che l'occupazione degli spazi sia coerente con quanto definito in fase di progettazione e regolare aspetti quali programmazione del funzionamento degli impianti termici e di illuminazione
- In fase di manutenzione

- Utilizzo dei modelli BIM per le operazioni di manutenzione dal campo e alimentazione del gemello digitale con i dati degli interventi effettuati
- Gestione delle anomalie tramite rilevamento dei dati da sensoristica installata nell'asset reale e loro confronto con i dati di riferimento previsti in fase di progettazione, con l'obiettivo di riscontrare discostamenti che potrebbero avere impatti più o meno importanti sull'opera reale (caso particolarmente interessante ne caso di infrastrutture, quali ponti, viadotti, ferrovie, …)

1.3.3. GAN (Generative Adversarial Networks)

Le reti neurali artificiali sono tecniche di apprendimento automatico con un legame ingresso-uscita, ispirato a strutture neuronali evolute e complesse, che a partire da un vettore n-dimensionale in input, che solitamente rappresenta una sollecitazione (i.e., segnali), permettono una variazione di tale input tramite funzioni non-lineari e elementi di calcolo elementare[15]. Le reti neurali artificiali possono essere impiegate per risolvere problemi di riduzione della dimensionalità di un dataset, classificazione e regressione. Nei problemi di classificazione, dove c'è la necessità di rappresentare un segnale con una classe di appartenenza, il comportamento del fenomeno fisico in input viene associato a una variabile a valori discreti, mentre nei problemi di regressione al comportamento del fenomeno fisico in input (descritto con valori reali variabili indipendenti) viene associata una variabile dipendente.

L'apprendimento automatico avviene tramite l'identificazione di un dataset di training avente un legame ingresso-uscita tra varabili – tali da descrivere il fenomeno in esame - applicando l'algoritmo di backpropagation[16] (retro-propagazione). L'algoritmo di retro-propagazione è un elemento essenziale nella fase di training, in quanto permette, ad ogni iterazione, di aggiornare i pesi (parametri delle reti neurali artificiali) per minimizzare l'errore.

[15] McCulloch, W.S., W. Pitts (1943), "A logical calculus of the ideas immanent in nervous activity," Bulletin of Mathematical Biophysics, vol. 5, pp. 115-133.
[16] Cilimkovic, M. (2015). Neural networks and back propagation algorithm. Institute of Technology Blanchardstown, Blanchardstown Road North Dublin, 15(1).

Ad oggi, esistono vari tipi di architetture di reti neurali artificiali[17], più o meno complesse. La complessità si basa sul numero, su come vengono posizionati e collegati tra loro gli elementi di calcolo elementare (i.e., "neuroni"). Ogni architettura viene utilizzata per risolvere problemi di diversa natura, in funzione della complessità del dataset di riferimento oggetto di apprendimento.

Tra le tante architetture di reti neurali artificiali troviamo le Generative Adversarial Networks (GAN)[18] che sono una classe di metodi generativi, in grado - per via di come sono collegati tra loro i vari elementi di calcolo elementare – di imparare le distribuzioni dai campioni reali prese in input dal dataset, per generare dati che assomigliano a quelli di un dataset di riferimento. L'idea alla base delle architetture GAN è quella di avere due reti neurali che possano essere in "competizione" tra loro così da ottenere un modello in grado di generare dati sintetici (come, ad esempio, immagini) tali da assomigliare ai dati presenti all'interno del dataset di riferimento. I dati sintetici sono una tipologia di dati prodotti artificialmente, tali da esprimere il comportamento di un fenomeno fisico più fedeli possibile da un punto di vista statistico.

La prima rete, chiamata generatore, crea dati sintetici cercando di imitare il dataset di riferimento. La seconda rete, chiamata discriminatore, cerca di distinguere i dati sintetici prodotti dal generatore dai dati reali del dataset di riferimento. L'obiettivo del generatore è quello di ingannare il discriminatore, creando dati sintetici sempre più simili ai dati reali, mentre l'obiettivo del discriminatore è quello di riuscire a distinguere sempre meglio tra i dati reali e quelli sintetici.

Il processo di addestramento di una GAN avviene attraverso l'algoritmo di "backpropagation" (retropropagazione dell'errore), pertanto prevede l'aggiornamento dei pesi delle reti neurali in modo da migliorare la capacità del generatore di generare dati sintetici sempre più simili ai dati reali e del discriminatore di distinguere tra i dati reali e quelli sintetici.

[17] Abiodun, O. I., Jantan, A., Omolara, A. E., Dada, K. V., Mohamed, N. A., & Arshad, H. (2018). State-of-the-art in artificial neural network applications: A survey. Heliyon, 4(11), e00938

[18] Creswell, A., White, T., Dumoulin, V., Arulkumaran, K., Sengupta, B., & Bharath, A. A. (2018). Generative adversarial networks: An overview. IEEE signal processing magazine, 35(1), 53-65.

Le GAN sono un tipo di rete neurale molto interessante per catturare effetti complessi, in particolare nel trattamento delle immagini X-RAY medicali[19] immagini per comprendere come evolve il cervello dei pazienti in presenza e assenza di patologie dirette. Un approccio molto interessante riguarda l'applicazione delle GAN su tumori multiformi del glioblastoma - il tipo più comune e aggressivo di tumori cerebrali primari – per comprenderne in anticipo l'evoluzione del tumore e prevedere una cura per il trattamento. Altre applicazioni in ambito medicale delle GAN su immagini, suppor ancora con qualche limitazione che potrà essere risolta e migliorata grazie alla ricerca e integrando dati aggiuntivi multi-omici e clinici, è nell'utilizzo di tali tecniche per la modellazione dello sviluppo (a) dell'invecchiamento del cervello, (b) progressione della malattia Alzheimer e (c) progressione delle lesioni celebrali (ad esempio in presenza di sclerosi multipla).

Ad oggi, la letteratura mostra come le GAN possono essere utilizzate anche per altre tipologie di applicazioni, meno nobili, ma non per questo di minore rilevanza e importanza. Il dominio di applicazione può essere:

- Dati Sintetici. Generazione di dati sintetici per migliorare i dataset già a disposizione e pertanto migliorare la qualità nella classificazione e previsione degli algoritmi di Machine Learning.
- Image inpainting. Ripristino di parti mancanti da immagini.
- Generazione di immagini. Creazione di immagini, conversione di immagini 2D in 3D, upscaling di immagini a bassa risoluzione ad alta risoluzione
- Image Denoising. Rimozione del rumore da immagini. Ad esempio, la rimozione del rumore statistico dalle immagini a raggi X in ambito sanitario

Questo tipo di reti possono essere utili per molti scopi benevoli, ma sicuramente un punto di attenzione riguarda il loro utilizzo per scopi malevoli, come la produzione di fake news o la rimozione di watermark da foto protette. Una sfida del prossimo futuro sarà individuare le circostanze di utilizzo non lecito degli algoritmi di AI, tra cui sicuramente le GAN, per evitare un uso improprio.

[19] Ghosheh, G., Li, J., & Zhu, T. (2022). A review of Generative Adversarial Networks for Electronic Health Records: applications, evaluation measures and data sources. arXiv preprint arXiv:2203.07018.

In sintesi, le GAN rappresentano uno dei più importanti sviluppi dell'Intelligenza artificiale degli ultimi anni, e sono destinate a diventare sempre più importanti per molte applicazioni in futuro. Tuttavia, è importante comprendere le sfide che si presentano nell'addestramento di queste reti neurali e come mitigare i rischi associati alla loro utilizzo.

1.3.4. Machine Learning Operations

L'Intelligenza artificiale (AI) è sempre di più percepita dalle aziende come un generatore di valore.

Fino a poco tempo fa, molte aziende che si occupavano di IA si concentravano principalmente su domande quali:

- Esistono aree o casi d'uso in cui possiamo creare valore dall'AI?
- Qual è il giusto approccio al modello per i casi d'uso identificati?
- Quale algoritmo dovremmo utilizzare?
- Quali dati dobbiamo raccogliere?

Tutte queste domande appartengono alla fase iniziale "sperimentale" del ciclo di vita di un'applicazione di IA. Sono tutte domande valide e fanno parte della sperimentazione scientifica empirica.

Per usare un'analogia di produzione: un conto è creare un prototipo estremamente efficace in fase di ricerca e sviluppo (R&S), ben altro è integrarlo all'interno di linee di assemblaggio altamente automatizzate

Molte organizzazioni hanno investito su prototipi di laboratorio (R&S) non tenendo però in considerazione la necessità di sviluppare un'infrastruttura e processi che consentissero una transizione dalla fase prototipale a quella di produzione di massa.

Pertanto, oggi solo un piccolo numero di aziende riesce a sfruttare il vero valore dei loro prototipi di machine learning (ML), e la maggior parte di queste aziende sta ancora affrontando il divario tra sperimentazione e produzione per le loro applicazioni di AI.

Approfondiremo di seguito le metodologie di MLOps, del perché le organizzazioni dovrebbero utilizzarle e quali siano le strategie per integrarle nei processi produttivi.

L'MLOps e i benefici derivanti

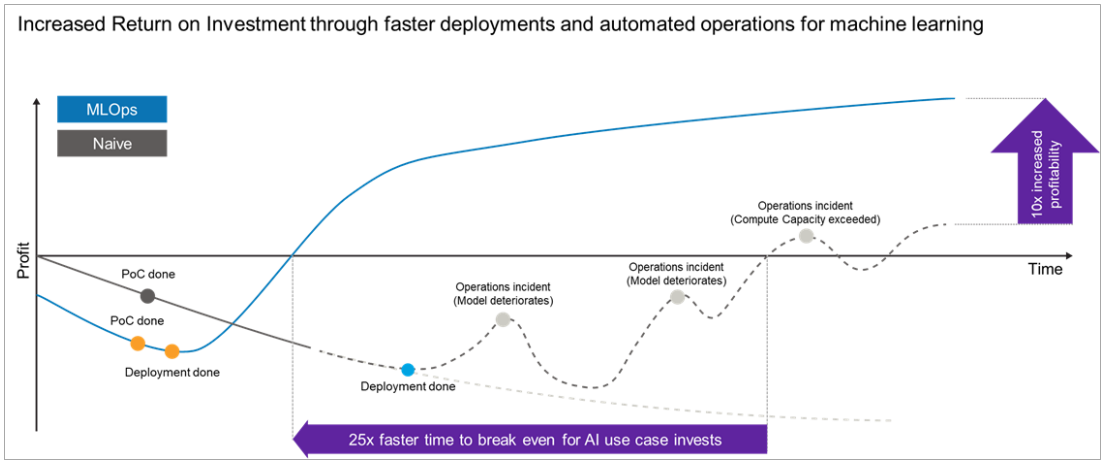
La soluzione per trarre un reale valore dai progetti di machine learning (ML)è introdurre il MLOps, acronimo di "Machine Learning Operations".

MLOps è una combinazione di pratiche, metodi di collaborazione e processi ed-to - end supportati da un framework tecnologico che consente di strutturare e automatizzare la gestione del ciclo di vita dei sistemi di machine learning e consente alle aziende di sviluppare, testare, distribuire, monitorare ed eseguire modelli di machine learning integrandoli nei processi aziendali in modo sicuro e veloce.

I principali benefici del MLops sono:

- Favorire la collaborazione tra le unità di business coinvolte;
- Ridurre il time-to-market per nuovi casi d'uso basati su AI;
- Abilitare la Trasparenza e verificabilità delle operazioni di machine learning;
- La creazione di sistemi robusti, affidabili e scalabili;

L'industrializzazione del modo in cui i modelli di ML vengono sviluppati, implementati e gestiti nel tempo ha un impatto significativo sul valore che tali modelli possono portare.



Figutra 10. Impatto di MLOps sui costi. Fonte: DXC

Come si può notare in figura, procedere in modo non organizzato ("naive"), senza l'implementazione delle pratiche e dell'infrastruttura MLOps, comporterà tempi di implementazione più lunghi e vari incidenti operativi con un incremento dei costi operativi e un ritardo nel raggiungimento del "break even".

Di seguito, si riporta uno schema sintetico delle più importanti best-practice dell'MLOps.

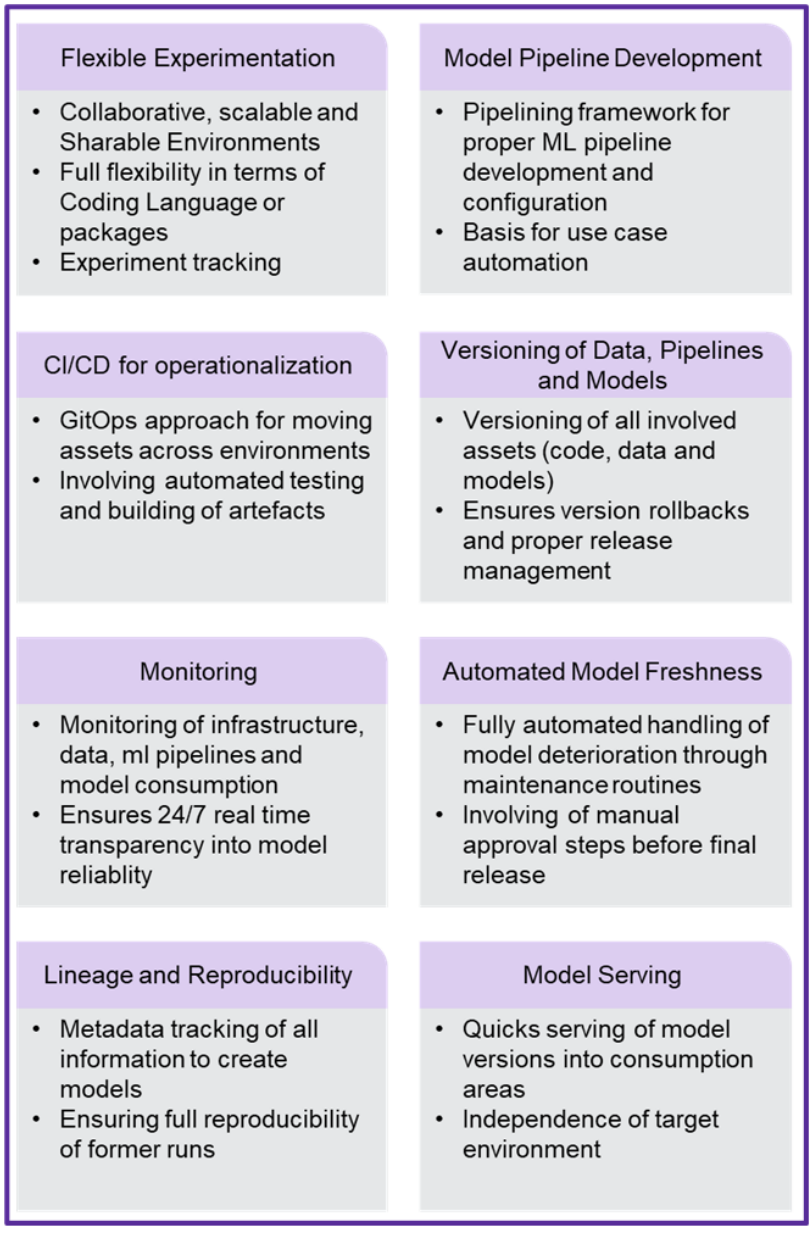


Figura 11. Best Practices in MLOps. Fonte: DXC

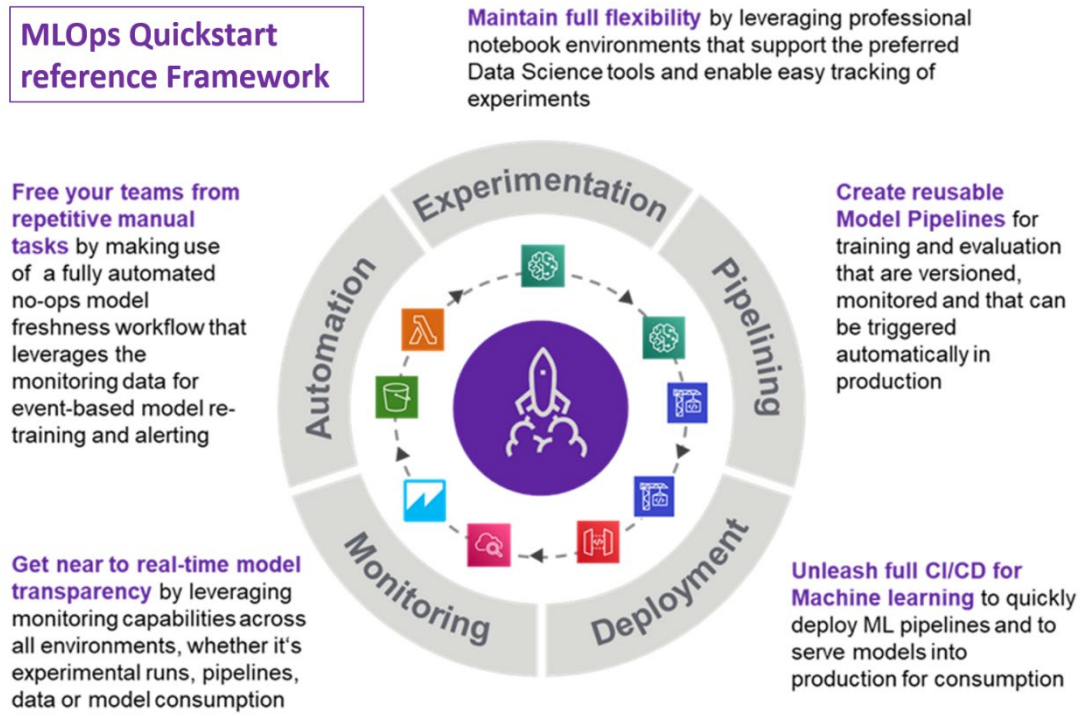
Con tempi di implementazione più rapidi e operazioni più stabili, MLOps consente di trarre valore dall'AI in tre modi:

1. Il beneficio della sperimentazione su nuovi casi d'uso viene finalmente raggiunto, poiché MLOps abilita l'introduzione dei nuovi modelli all'interno dei processi aziendali;

2. I costi di implementazione e di esercizio dei modelli di ML vengono drasticamente ridotti, spesso fino al 75%.
3. La realizzazione di applicazioni IA affidabili favorisce una cultura di innovazione in cui l'IA è vista come parte integrante dei processi aziendali favorendo la creazione di nuovi modelli.

Nel seguito del paragrafo, si illustra un possibile framework concettuale che possa guidare le aziende nell'adozione ed applicazione dell'MLOps all'interno dei propri processi produttivi.

Di seguito una figura di sintesi della soluzione proposta.



Figutra 12. Schema di adozione di MLOps nei processi produttivi

In dettaglio, segue una descrizione dei principali componenti del framework:

- *Memorizzazione delle feature (Feature storage)*

Dal momento che i dati rappresentano il carburante delle applicazioni AI, lo sviluppo end-to-end dell'AI implica la progettazione e l'implementazione di pipeline dati stabili e monitorate. Tuttavia, per mantenere una modularità e

separare i dati dall'architettura MLOps, i feature store fungono da interfaccia tra i due domini.

Per grandi progetti di AI, i feature store offrono una singola fonte di dati per lo sviluppo del machine learning e garantiscono che le caratteristiche sviluppate siano riutilizzabili e non incorporate nel codice specifico di un caso d'uso particolare.

- *Sperimentazione flessibile*

Sebbene MLOps si concentri sulla distribuzione e sull'operatività, i Data Scientist hanno bisogno di flessibilità per eseguire esperimenti nei loro ambienti e framework di strumenti preferiti. Per garantire ciò, assicurandosi allo stesso tempo che i data scientist lavorino in ambienti pronti per la produzione, si propone di sfruttare notebook containerizzati e ambienti di sviluppo integrati (IDE) che siano versionati, condivisibili e scalabili.

- *Repository dei modelli*

La riproducibilità è fondamentale per garantire che la qualità del modello sia mantenuta nel tempo. Pertanto, si eseguono run di training del modello orchestrati e completamente registrati sia in fase di sviluppo che di produzione. Ciò garantisce che tutti gli aspetti di un modello siano memorizzati, indipendentemente dal fatto che vengano utilizzati in seguito in produzione, e consente un'adeguata comparazione del modello nel tempo e su vari set di training e di validazione.

- *Sviluppo della pipeline di ML*

La distribuzione basica (naive) del modello si concentra sulla distribuzione diretta dei singoli modelli in produzione. Questo approccio non tiene conto del fatto che il degrado delle performance del modello non costituisca un evento raro ma la norma. Ci si deve aspettare sempre un frequente riaddestramento del modello. Pertanto, non è il modello che deve essere distribuito in produzione ma le pipeline di training del modello. Queste pipeline di modellazione, attivate da determinate condizioni come l'arrivo di nuovi dati etichettati, addestreranno, testeranno e compareranno automaticamente le nuove versioni del modello, se necessario.

- *CI/CD per la distribuzione della pipeline di ML*

Per minimizzare lo sforzo manuale, la distribuzione della pipeline del modello viene eseguita con l'aiuto di pipeline CI/CD (Continuous Integration/Continuous Delivery).

- *Distribuzione del modello*

Con le pipeline di training attivate automaticamente, nuove versioni completamente registrate del modello saranno disponibili nel repository dei modelli. Agganciarle ai servizi predittivi può essere automatizzato o eseguito dopo l'approvazione manuale.

Questo approccio consente agli utenti di progettare test utili a confrontare le prestazioni reali nel tempo, relative a diversi modelli in produzione.

- *Monitoraggio del modello*

L'esecuzione dei modelli di ML in produzione richiede un monitoraggio attento delle loro prestazioni. A seconda del caso d'uso e del modello di servizio, è necessario sviluppare delle soluzioni di monitoraggio adeguate. In generale, il monitoraggio del modello comporta almeno due livelli:

1. Il monitoraggio del servizio predittivo richiede il tracciamento dello stato del servizio, il numero di richieste e l'output del modello;
2. Il monitoraggio delle prestazioni del modello, all'arrivo di nuovi dati etichettati, richiede la valutazione del modello di produzione corrente dei nuovi dati. Il monitoraggio dei flussi di dati coinvolti garantisce la validazione della qualità dei dati in tempo reale.

2. PARTE SECONDA – MERCATO DELL'IA

La seconda parte del White Paper tratta del tema del *Mercato* delle soluzioni di Intelligenza artificiale[21]. Secondo il Rapporto "Il Digitale in Italia 2023 vol.1" il mercato italiano IA si è attestato nel 2022 a 435 milioni di euro, in crescita di oltre il 32% rispetto al 2021. Per il 2023 è stimato un volume di 570 milioni di euro che indica un tasso di crescita ancora superiore al 30% (31%). Tra il 2020 – anno della crisi pandemica – e il 2023 il mercato è più che raddoppiato (+128%). Nei prossimi anni, il mercato IA manterrà questo altissimo ritmo di crescita. Infatti, si stima che tra il 2022 e il 2026 il tasso di crescita annuo medio del mercato IA sarà del 28,9% portandolo al volume di 1,2 miliardi di euro nel 2026.

21

Nel perimetro di mercato dell'Intelligenza artificiale sono incluse le componenti hardware, software e servizi professionali nell'ambito delle seguenti soluzioni

- Intelligent Data Processing
- Natural Language Processing/IA generativa
- Recommendation Systems
- Computer Vision / Data Visualization
- Chatbot / Assistenti Virtuali
- Robotic Process Automation/ Intelligent Automation

In particolare l'Intelligenza artificiale generativa rappresenta un'evoluzione dell'NPL e include algoritmi basati su modelli matematici addestrati su enormi quantità di dati e con la capacità di generare autonomamente contenuti originali ed estremamente realistici di diversa natura (musicali, audio, software, immagini, testo e video).

Nel perimetro sono considerate le sole soluzioni utilizzate in ambito business da parte di imprese private o enti pubblici. Non sono considerate nel mercato IA apparati "general purpose" utilizzate nel segmento consumer quali Alexa e Siri. Tali apparati sono invece inclusi per la quota utilizzata nell'ambito di applicazioni professionali (ad es in Sanità per il tele-monitoraggio)

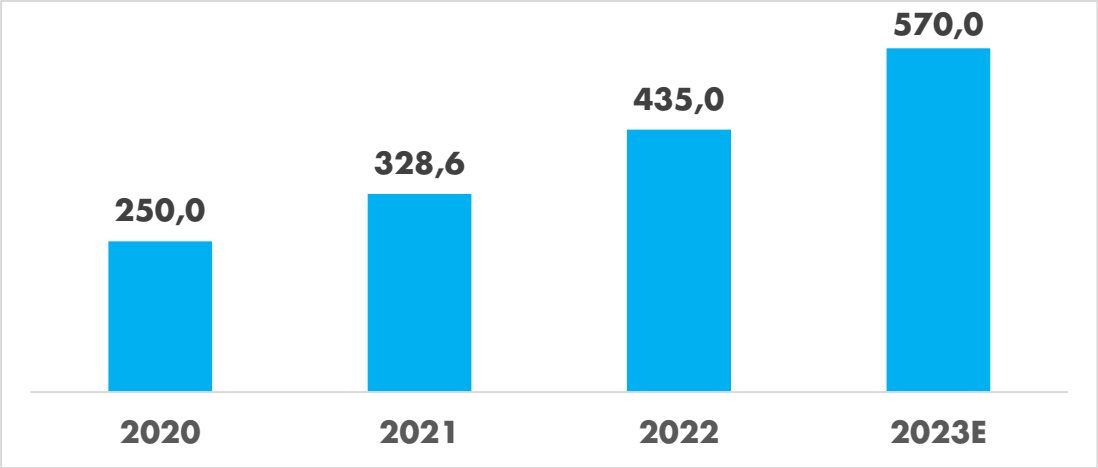


Figura 13. Volume del Mercato IA in Italia. Fonte: NetConsulting Cube 2023

Nonostante l'elevato tasso di crescita, il mercato mostra ancora un volume abbastanza contenuto. In Italia l'Intelligenza artificiale rimane ancora scarsamente utilizzata dalle aziende, soprattutto nel segmento PMI. Secondo dati ISTAT del 2021, solo il 6,2% delle imprese con almeno 10 dipendenti ha dichiarato di utilizzare sistemi di Intelligenza artificiale, contro una media dell'8% nell'Unione europea; in particolare, la percentuale di piccole imprese (10-49 addetti) si attesta al 5,3%, contro il 24,3% delle grandi imprese (250 e più addetti). Nel paragrafo offriremo una "fotografia" del mercato italiano e delle recenti tendenze di sviluppo.

2.1. IA nei macrosettori economici

Per quanto riguarda i settori economici, le aree di maggiore sperimentazione per l'IA sono sicuramente nel *banking* e nel mondo *telco e media* (Fig 13). Entrambi i settori presentano un volume di mercato IA relativamente elevato (>80 mln) e un tasso di crescita superiore al 30%. Alcuni settori, come trasporti, utilities e servizi, hanno volume medio (30-40 mln) e una crescita più lenta rispetto alla media (<30%), mentre Sanità, Industria e assicurazioni presentano elevati tassi di crescita (>35%) e buon volume di mercato (30-50 mln). Più indietro invece il settore della Pubblica Amministrazione, con la PA Centrale più rilevante in termini di spesa rispetto alla PA Locale. Il settore pubblico sconta un ritardo dovuto a un mercato ancora immaturo (5-15 mln circa) ma presenta tassi crescita molto elevati (36 e 37% rispettivamente).

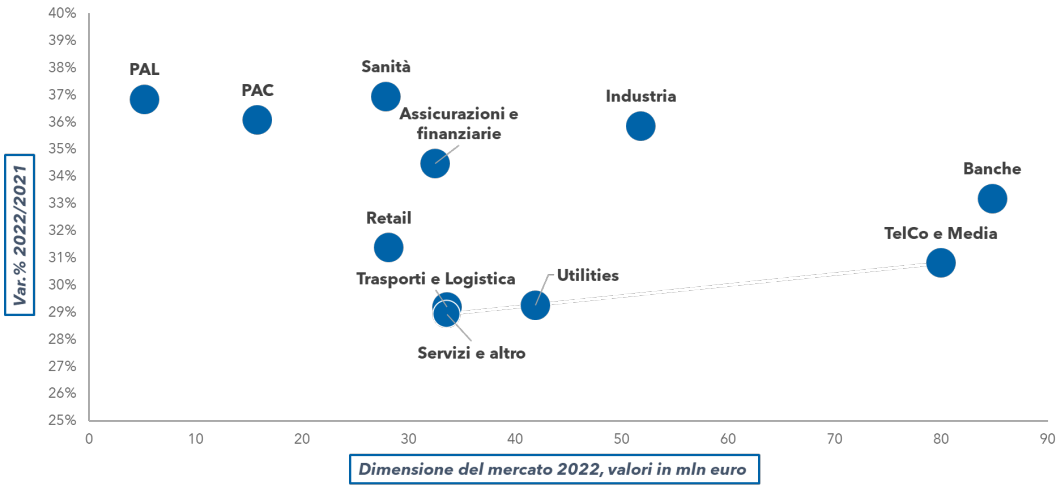


Figura 14. Mercato IA italiano per macrosettore economico. Fonte: Netconsulting Cube.

2.2. I trend di investimento nel 2023: chi investirà e dove?

L'indagine svolta da NetConsulting ci permette di avere un quadro chiaro sulle *previsioni di investimento in IA nel 2023* e sulla *distribuzione degli investimenti per diverse tipologie*. Per quanto riguarda le previsioni (Fig. 14) è stato chiesto a un campione di aziende provenienti da vari settori se intendono avviare investimenti in IA nel 2023; per la distribuzione per tipologie si sono considerate le varie tecnologie del perimetro dell'IA (Intelligent Data Processing, Natural Language Processing, Recommendation Systems, Computer Vision / Data Visualization, Chatbot / Assistenti Virtuali, Robotic Process Automation/ Intelligent Automation) utilizzate da parte delle aziende che già hanno adottato soluzioni di IA (Fig. 15).

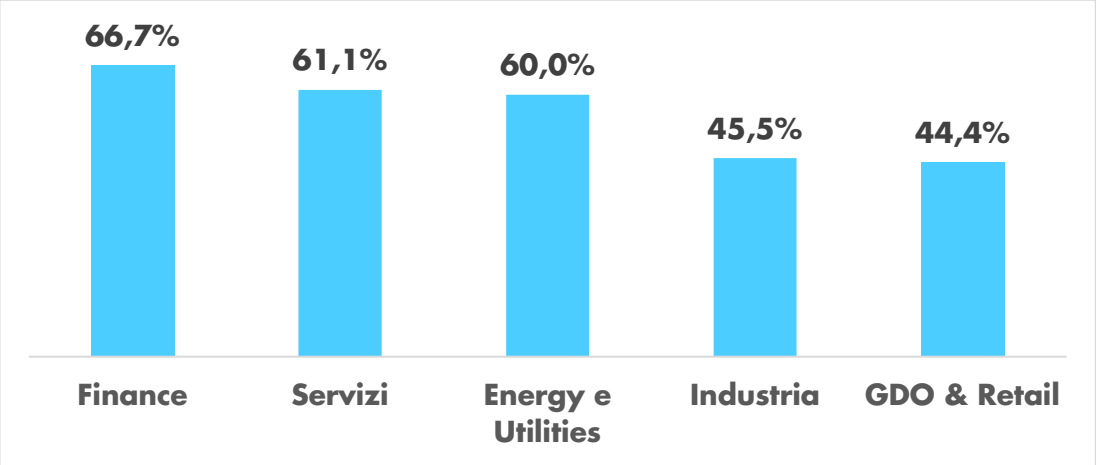


Fig. 15. Previsioni di investimento in IA, 2023 – focus settoriale. Dati in % sul totale delle delle aziende intervistate.

Due terzi delle aziende del *Finance* intervistate e il 60% di quelle dei servizi prevedono investimenti in IA, più caute invece le aziende dell'industria (45,5%) e di grande distribuzione e retail(44,4%).

Per quanto riguarda le singole tecnologie IA, tra il 2022 e il 2023 si osserva un incremento soprattutto in Intelligent data processing, Natural language processing e Chatbot (Fig. 15). L'RPA (Robotic Process Automation) è il principale tipo di soluzione nell'industria, nel *finance,* in grande distribuzione e retail e Energy. I servizi, invece, utilizzano maggiormente Chatbot e assistenti virtuali (vista l'importanza dell'interazione con il cliente).

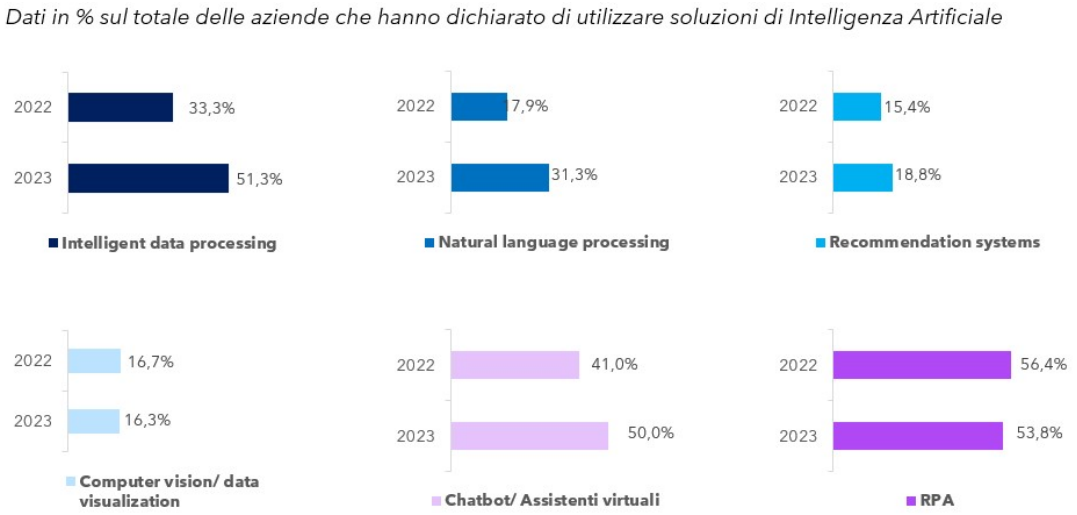


Fig. 16. Concentrazione degli investimenti in soluzioni di Intelligenza artificiale. Fonte NetConsulting Cube 2023.

Complessivamente tra il 2022 e il 2023 crescerà in modo significativo l'*uptake* di soluzioni di IA in azienda, sia per numero di aziende che per intensità di utilizzo. Come illustra la figura 17, la quota di aziende che indicano un utilizzo importante dell'IA in molti processi passerà dal 4% al 14%, così come la quota di aziende che non utilizzano l'IA o la utilizzano in minima parte, diminuirà sensibilmente.

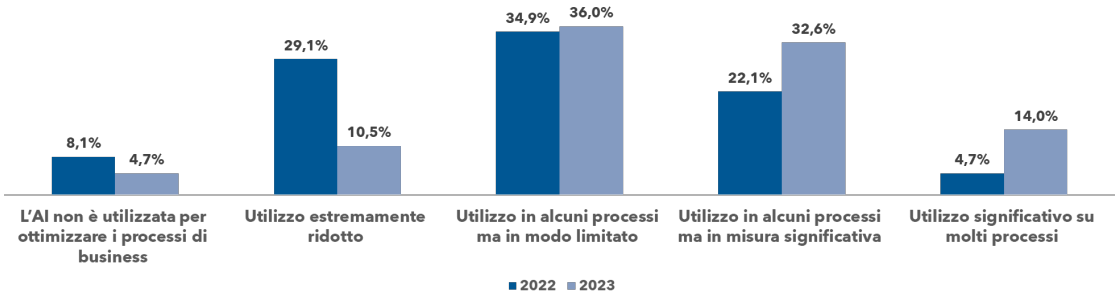


Fig. 17. Grado di utilizzo dell'Intelligenza artificiale per l'ottimizzazione dei processi di business. Fonte: NetConsulting Cube 2023.

I dati sull'adozione, per settore e tipo soluzione, restituiscono un panorama dinamico, con un'adozione in forte crescita in diversi settori.

Dato il contesto descritto, le successive sezioni del White Paper forniranno numerosi esempi di utilizzo di IA in azienda e di scenari di applicazione in settori verticali.

3. PARTE TERZA – UTILIZZO DELL'IA

Questa parte raccoglie un insieme di casi d'uso originati dalle aziende partecipanti al Gruppo di Lavoro e ulteriori case study che si sono evidenziati negli incontri organizzati sul territorio.

3.1. Telecomunicazioni (TIM)

Le reti di nuova generazione, che comprendono l'FTTH, il 5G e la sua evoluzione verso il 6G prevista al 2030, sono caratterizzate da architetture sempre più cloud based e open che registrano il superamento graduale del modello di rete a nodi discreti basati su standard chiusi del mondo TLC ("black boxes").

In parallelo il trasferimento dell'Intelligenza artificiale da cloud centralizzati alla periferia della rete (edge cloud) permette ancor più l'utilizzo delle informazioni in tempo reale a vantaggio dell'industria e della società.

Esiste uno stretto legame tra la diffusione di sistemi basati sull'Intelligenza artificiale e lo sviluppo di reti di comunicazione (in particolare 5G) in grado di collegare svariati dispositivi, raccogliere dati ed utilizzare le informazioni su larga scala per il miglioramento di infrastrutture, sistemi, processi e servizi.

Le reti di telecomunicazioni saranno sempre più caratterizzate da un crescente livello di automazione, sia per favorire maggior efficienza ed efficacia nella loro gestione che per favorire la creazione di servizi digitali con cicli di innovazione più brevi, i cui servizi vengono offerti al mercato in modalità "*as a service*" tramite APIs (Application Programming Interface) di rete, secondo il modello di successo usato per creare apps sugli smartphones.

In questo scenario l'Intelligenza artificiale riveste un ruolo sempre più importante, sia nella parte di progettazione delle reti che nei processi operativi di gestione delle stesse che ad oggi sono ancora fortemente human driven. L'utilizzo dell'automazione intelligente consente di riservare e concentrare le interazioni personali su attività più complesse che richiedono empatia umana, creatività o giudizio - in altre parole, sui lavori che non possono essere automatizzati.

L'IA applicata alle reti verrà alimentata da una enorme mole di dati provenienti dagli apparati ma anche dai clienti, per coniugare lo sviluppo della rete con le aspettative degli utenti in termini di mobilità, banda e altre caratteristiche dei servizi digitali utilizzati. Le elevate bande delle reti in fibra e del 5G e l'estensione delle telecomunicazioni al mondo degli oggetti secondo il paradigma *Internet of Things* (IoT) rende disponibile un flusso di dati in crescita esponenziale permettendo ai sistemi di Intelligenza artificiale di migliorare continuamente la user experience degli utenti, ridurre i costi operativi di rete per gli operatori e rendere le infrastrutture più sostenibili dal punto di vista ambientale. I sistemi basati su IA favoriscono nuovi "use case" nei settori IoT, business intelligence, robotica industriale, trasporto intelligente, realtà virtuale e altro ancora.

L'Intelligenza artificiale permette l'automazione di molte attività come configurazione dei dispositivi, provisioning, manutenzione e la risoluzione dei guasti, gestione più snella dei "profili utente", prestazioni più elevate e implementazione più rapida di nuovi servizi, proponendo quelli più idonei in base al comportamento dinamico dei clienti.

L'uso di questi dati per l'IA si basa su una regolamentazione molto stringente, che vede gli operatori non solo ottemperare a regolamentazione di tipo orizzontale (es. GDPR) ma anche a regolamentazione verticale (es ePrivacy directive), che caratterizzano le telecomunicazioni in Italia ed in Europa.

3.1.1. Pianificazione di rete con il supporto dell'AI

La pianificazione delle reti mobili è finalizzata al raggiungimento della miglior copertura possibile del territorio in rapporto alle aspettative degli utenti, unita ad una ottimale capacità di smaltimento del traffico generato dai servizi utilizzati. È un problema complesso e multidimensionale di elaborazione dei parametri delle celle che si presta particolarmente bene per essere risolto da algoritmi di Intelligenza artificiale. Ad esempio, nella pianificazione dei tilt delle antenne che generano localmente la copertura radiomobile l'IA porta miglioramenti significativi rispetto agli algoritmi attualmente in uso.

L'IA abilita aggiustamenti dinamici della configurazione di rete adattandone le caratteristiche alla evoluzione dell'uso che ne fanno gli utenti, in maniera più efficiente di quanto fatto sino ad ora.

Su questo TIM ha effettuato nel 2021 un importante progetto pilota nel comune di Fossano, caratterizzato da un'area comunale complessa di circa 130 chilometri quadrati dove oltre al centro cittadino ad alta densità abitativa sono presenti vari stabilimenti produttivi, una zona collinare e un'ampia superficie dedicata alle coltivazioni. Con l'impiego dell'IA, in particolare di **Eris** (Enhanced reinforcement learning for innovating self organizing networks) e con il supporto della tecnologia Ret (Remote electrical tilt) è stato ottenuto un miglioramento prestazionale compreso tra il 10% e il 20% nei siti più congestionati appartenenti al territorio (circa 130 antenne). La tecnologia Ret ha consentito di regolare a distanza l'inclinazione delle antenne montate sulle torri rispetto al terreno, al fine di ottenere la portata (throughput) ideale. Il diagramma di irradiazione viene ottimizzato per alleggerire i siti più stressati sfruttando le risorse, oggi sottoutilizzate, di altri siti.

Eris è capace di imparare da sé e, a fronte di miliardi di potenziali soluzioni alternative, esplora solo le più promettenti che la portano rapidamente ad individuare la soluzione ottimale.

Si tratta di reinforcement learning, ovvero apprendimento per rinforzo, una declinazione del generico machine learning - che a sua volta rappresenta una categoria dell'Intelligenza artificiale.

Nel caso dell'algoritmo in questione l'obiettivo da raggiungere è quello dell'efficienza; l'apprendimento per rinforzo avviene quindi combinando tutte le variabili degli scenari di rete possibili.

Si tratta di un importante elemento di innovazione e sostenibilità energetica.

3.1.2. Assurance di rete con il supporto dell'AI

La gestione operativa di rete finalizzata ad offrire un servizio ottimale agli utenti prevede la supervisione degli allarmi e quindi la gestione delle anomalie in maniera sempre più tempestiva. L'automazione basata su sistemi di Intelligenza artificiale può essere rilevante, ad esempio, quando i dati grezzi non sono strutturati in modo ordinato e assumono forme diverse o provengono da diversi ambienti software.

L'AI permette una forte ottimizzazione della gestione delle anomalie di rete automatizzando un processo ancora fortemente legato all'intervento umano. La

nuova frontiera dell'IA applicata alle reti è quella della *predictive maintenance*, ovvero la capacità di prevedere i guasti di reti sulla base delle esperienze pregresse con il fine di prevenirle minimizzando l'intervento dei tecnici sul territorio.

Le applicazioni basate sull'Intelligenza artificiale permettono infatti di passare dalla risoluzione reattiva delle anomalie a quella proattiva. Queste applicazioni sono infatti in grado di valutare grandi volumi di dati e apportare correttivi prima che le anomalie siano avvertite dagli utilizzatori dei singoli servizi o applicazioni.

La risoluzione anticipata dei guasti e dei disservizi migliora la disponibilità del servizio e conseguentemente la costumer experience e la soddisfazione dei clienti, oltre a offrire una soluzione all'intervento rapido in situazioni critiche.

L'Intelligenza artificiale ha quindi un ruolo anche nell'individuazione delle attività necessarie, sulla base dei dati analizzati e nella gestione della loro esecuzione, "chiudendo" i processi di manutenzione all'interno della rete.

Il suo uso applicato ai dati delle reti mobili sarà strumentale anche ad un utilizzo sempre più orientato al bene comune. L'analisi profonda delle aspettative degli utenti per progettare le smart cities, il supporto alla protezione civile in caso di disastri ambientali rilevando in maniera più precisa i segnali deboli dei cellulari, e l'analisi dei pattern di uso dei servizi per migliorare il welfare diventeranno sempre più diffusi nel contesto di partnership pubblico private tra PA/PAL ed operatori.

3.2. Human Resources (Mylia)

3.2.1. Fotografare la complessità organizzativa: strumenti di machine learning per una lettura del comportamento in chiave reticolare

L'attuale scenario incerto e dinamico richiede una lettura della complessità e del comportamento organizzativo in una prospettiva sistemica. La nostra ricerca offre un contributo all'analisi della complessità organizzativa attraverso una fotografia multidimesionale del comportamento. Il metodo utilizzato si avvale di strumenti di machine learning per rilevare le interconnessioni tra i comportamenti agiti da una persona all'interno del suo contesto operativo. Il disegno di ricerca ha visto come prima fase la costruzione di un modello di

lettura del comportamento organizzativo e del relativo strumento di rilevazione, l'elaborazione di una metodologia di analisi dei dati, l'utilizzo di strumenti di machine learning per concludersi con la fase di data visualization. Il nostro modello di lettura del comportamento organizzativo nasce dal confronto tra le teorie di riferimento presenti in letteratura e l'esperienza pratica maturata sul campo. Si articola in 4 aree e 16 comportamenti che hanno guidato la scelta di indicatori e item associati per la costruzione del questionario. Nello scegliere la metodologia di analisi dei dati con l'obiettivo di rilevare le interconnessioni tra i comportamenti, abbiamo integrato l'analisi univariata con una tecnica multivariata basata sull'applicazione di strumenti di Machine Learning. Questo ha consentito al team di realizzare una fotografia reticolare ad alta risoluzione attraverso tre attività specifiche:

- creazione di una topologia multidimensionale basata su una Mappa di Kohonen (una tipologia di rete neurale artificiale ad apprendimento non supervisionato), volta a rappresentare geometricamente le relazioni tra i comportamenti;
- implementazione del metodo di cluster analysis, k-means, per l'individuazione di aree della mappa caratterizzate da fattori di similarità o affinità nel comportamento;
- individuazione della posizione delle persone all'interno della mappa e dei vari cluster individuati.

La ricerca ha messo in evidenza la validità degli strumenti di machine learning per rilevare la multidimensionalità del comportamento organizzativo. Questo ci ha permesso di valorizzare la logica reticolare tra i vari elementi osservati e di **visualizzare una complessità altrimenti non accessibile attraverso una reportistica multimediale e interattiva**.

L'applicazione sul campo della ricerca è avvenuta tramite la progettazione e lo sviluppo di un prototipo integrato ad una piattaforma LMS attraverso un plug in. In questo modo abbiamo avuto una conferma sull'efficacia del metodo per la costruzione di percorsi di crescita professionale/sviluppo. Questa sperimentazione, inoltre, ci ha consentito di ottenere dati significativi dovuti all'applicazione del nostro modello a diversi settori, in particolare nel settore Farmaceutico, TLC, Banking, Automotive, Machinary, Servizi. In un caso specifico ci siamo trovati a lavorare con un'azienda del settore Automotive, che

aveva manifestato il bisogno di realizzare una fotografia dei diversi stili manageriali del proprio Management Team per:

- identificare le tendenze comuni ed eventuali aree di attenzione;
- osservare il modello prevalente di managerialità;
- valorizzare la diversità di approccio manageriale;
- riconoscere le priorità di sviluppo per il gruppo;
- focalizzare le aree principali di necessità per un intervento del gruppo sul contesto organizzativo.

Il nostro obiettivo a fronte di questa richiesta- ma in generale quando dobbiamo affrontare sfide di sviluppo- è stato quello di fornire una "fotografia intelligente" della managerialità attraverso una rappresentazione grafica dei comportamenti funzionali ai processi organizzativi da parte del team mappato.

Il grande vantaggio di utilizzare mappe intelligenti è quello di poter usufruire di un apprendimento non supervisionato per produrre la rappresentazione del campione in uno spazio preservandone le proprietà topologiche.

Abbiamo utilizzato una tecnica di apprendimento automatico che consiste nel fornire al sistema informatico una serie di input che egli ha riclassificato e organizzato sulla base di caratteristiche comuni per cercare di effettuare ragionamenti e previsioni sugli input successivi, senza alcuna graduatoria arbitraria. Ottenendo quindi un sistema che si auto- organizza.

Aver avuto la possibilità, attraverso questo modello di lettura reticolare, di poter cogliere le relazioni tra i comportamenti e le loro interconnessioni, ha rappresentato un'importante opportunità per la funzione HR di acquisire **consapevolezza e dati** relativi a:

- **come sono espresse le energie manageriali** in risposta agli stimoli e alle richieste del contesto organizzativo.
- quali fossero **gli orientamenti manageriali del gruppo** identificandone i comportamenti maggiormente agiti e quelli meno presenti nel quotidiano del team

I flussi dei Comportamenti emersi -distribuiti in funzione della loro intensità di azione a seguito della loro interazione- si sono collocati all'interno di 9 Sottozone tra le 14 evidenziate nel campione di riferimento. I comportamenti maggiormente agiti dal gruppo descrivono un approccio manageriale che

impatta sul proprio contesto organizzativo attraverso ed in funzione degli obiettivi da raggiungere e delle attività da svolgere. La concentrazione dei manager in alcune di Sottozone rende le stesse più significative nel leggere gli orientamenti del gruppo e nell'identificare gli stili prevalenti di managerialità.

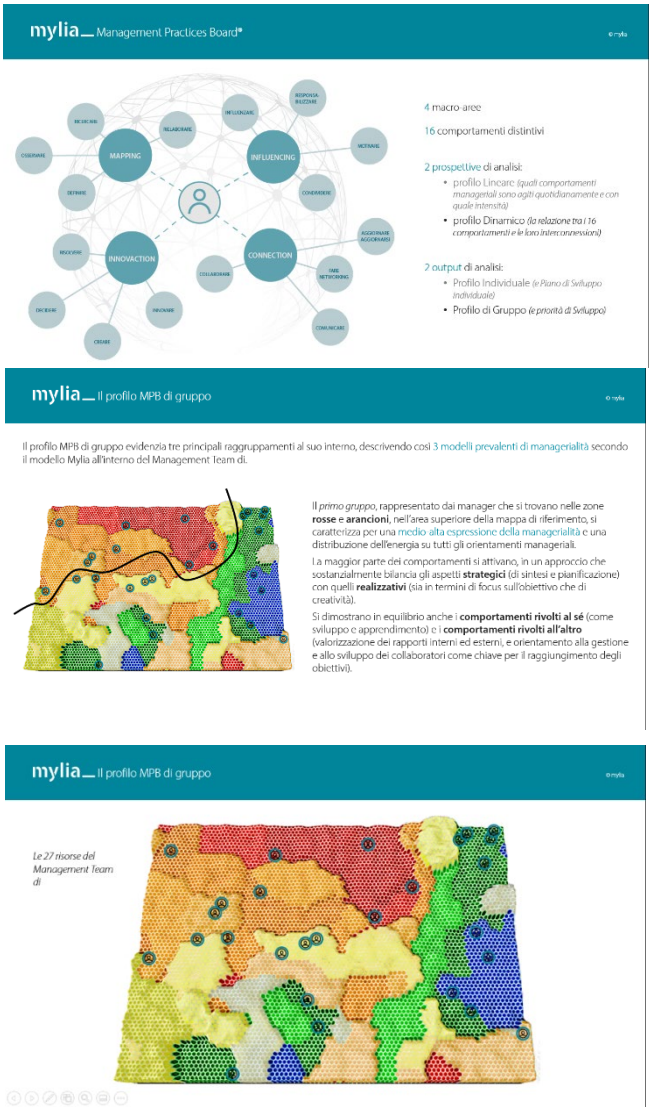


Figure 18a, 18b e 18c. Fonte: Mylia

Questa mappatura ha poi consentito di accompagnare il Management Team nell'effettivo sviluppo di un'abitudine funzionale al confronto e alla condivisione, attraverso la realizzazione di un piando di sviluppo sul medio periodo.

Gli incontri programmati hanno dato al team l'occasione di lavorare insieme concretamente sia sul gruppo stesso *(in particolare sulle dimensioni della managerialità identificate come prioritarie in termini di sviluppo)* sia su dinamiche e problematiche di natura più operativa (*ad esempio iniziative interfunzionali, processi di lavoro condivisi, attività di knowledge sharing, ecc.)*.

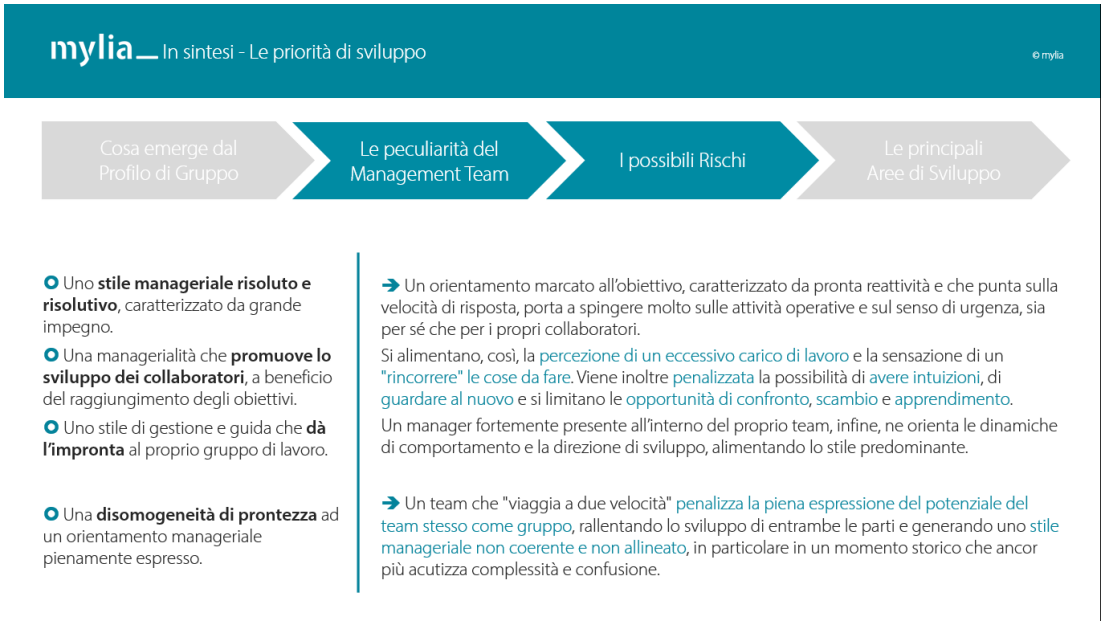


Figura 19. Fonte: Mylia

I vantaggi di questa azione di sviluppo:

- esercitare una visione di lungo periodo che, al momento, non trova espressione per il Management Team;
- rispondere al bisogno dichiarato da tutti di avere momenti di scambio e confronto utili a fare il punto con regolarità;
- cementare l'entusiasmo suscitato dalla situazione di confronto "forzato" che il colloquio di restituzione ha saputo creare;
- allenare l'abitudine ad incontrarsi come gruppo, limitando l'inevitabile "effetto abbandono" legato alla pressione dell'operatività;
- "abilitare" dall'alto la possibilità e l'utilità di ritagliarsi momenti dedicati allo scambio reciproco, al di fuori dell'operatività stessa

3.2.2. Data processing e recommendations engine per calcolare e orientare la impiegabilità di un profilo

Oggi il mercato propone diverse soluzioni (free, freemium, on demand, SAS, ecc.), piattaforme, software per effettuare un orientamento al mercato del lavoro sulla base di caratteristiche curriculari. Alcuni tool sono rilevanti per una analisi dei c.v., altri per esporre offerte formative coerenti con le aspirazioni professionali, talvolta mediate da quick assessment on line, altri ancora per consentire maggior consapevolezza nella scelta di un'offerta di lavoro o per veicolare quelle che rappresentino un match maggiore con il background formativo del candidato.

In questa sede lo use case che viene proposto è relativo all'identificazione (calcolo) di un indice di occupabilità, cioè la misurazione della capacità di una persona di rendersi occupabile rispetto a una determinata professione, come risultato dell'integrazione di due distinte componenti che a loro volta sono il risultato di fattori diversi.

Le due componenti sono:

- la richiesta di mercato - che è determinata dal numero totale di offerte di lavoro proposte a livello europeo per una specifica professione, dalla qualità del loro profilo contrattuale e dalla frequenza con la quale la domanda per quella specifica professione si protrae nel tempo –
- la copertura del ruolo - che è determinata dall'esperienza professionale della singola persona, dai titoli di studio conseguiti, dalle competenze specifiche (hard skills), da quelle trasversali (soft skills) e dalle sue competenze informatiche e di comunicazione.

Per poter svolgere questo lavoro in particolare, la piattaforma (denominata PHYD) deve mappare un cospicuo atlante delle professioni: nel nostro case ne mappa 2980, declinate su più di 20.000 denominazioni diverse e similari e oltre 19.000 competenze, rispettando gli standard internazionali determinati dai database Esco (per l'Europa) e O*Net (per il Nordamerica).

Inoltre, per poter prevenire processi di obsolescenza in questo specifico orientamento tramite l'identificazione dell'**employabiliy index,** il motore algoritmico processa i dati riguardanti la pubblicazione di offerte di lavoro e

quelli connessi ai livelli salariali, in modo da disporre di un quadro informativo completo e orientare così al meglio l'utente in maniera organica.

Gli elementi che il sistema deve poter mettere in correlazione – ed è questa la principale chiave di lettura e funzione d'uso dello use case – sono gli obiettivi professionali dell'individuo ovvero l'ambizione a ricoprire un determinato ruolo, la domanda reale del mercato, le competenze dell'individuo.

In termini più ampi, l'IA da un lato verifica quali saranno i lavori più richiesti nel prossimo futuro, quali competenze li abilita, e quali settori, già oggi, generano il maggior numero di opportunità professionali.

L'ulteriore funzione d'uso del motore è la capacità di fare recommendation rispetto a qualsivoglia percorso o iniziativa di formazione e sviluppo che sia accessibile e funzionale alla riduzione della distanza rispetto ai profili target da parte dell'individuo che interroga la piattaforma.

La piattaforma ha integrato diversi database che mette in relazione attraverso degli algoritmi proprietari.

Ogni professione ha un numero elevato di competenze ed ognuna è valorizzata secondo un livello minimo richiesto.

Le 2900 professioni ESCO sono state mappate e integrate con il DataBase Onet.

Applicazioni concrete che possiamo citare all'interno di questo use case sono almeno 3:

- L'utente che si affaccia al mercato del lavoro e necessita di avere una guida che lo supporti attraverso i servizi offerti per migliorare la propria consapevolezza e capire in base alle proprie competenze, testabili sia in autovalutazione che con gli assessment caricati in piattaforma, per quali ruoli è maggiormente pronto
- L'azienda che vuole comprendere:
    - come è posizionato il proprio capitale umano rispetto alla richiesta minima di mercato,
    - su quali ruoli le proprie persone potrebbero essere pronte e quali percorsi formativi sono necessari
- Le università, per aiutare gli studenti ad orientarsi post lauream.

Analizzando il caso aziende, il servizio PaaS è stato reso personalizzabile sviluppando un sistema che permette di nascondere alcuni moduli presenti (tra cui i tutor, selezionare i test e i provider di formazione) per rendere l'obiettivo aziendale il più possibile coerente con le aspettative.

I consulenti, una volta stabilito con il committente quali siano le professioni da mappare, hanno la facoltà di crearne di nuove (che saranno visibili solo nel tenant del cliente senza che ciò vada a sporcare i database internazionali), associando ad esse nuove competenze verticali per il committente, o cambiando il livello minimo atteso per ognuna di esse.

La personalizzazione è molto importante ai fini della valutazione attraverso i test che possono essere integrati e resi esclusivi per la committenza stessa.

Il motore di raccomandazione dei corsi e dei ruoli correlati partirà dalle nuove professioni inserite cercando ciò che è più congruente sia per suggerire di testarsi su ruoli sia per approfondire con i corsi migliori.

I corsi presenti sono sia caricati in un LMS che aggregati dal web.

Ogni volta che un utente conclude con successo il corso, le competenze correlate ad esso e valorizzate verranno inserite del profilo dell'utente stesso.

L'azienda grazie all'accesso come amministratore di sistema potrà vedere per ogni collaboratore i progressi fatti e, utilizzando una dashboard di PowerBI, comprendere come si stanno muovendo rispetto all'obiettivo i collaboratori che utilizzano il portale.

La piattaforma ha 3 database su cui girano tutte le informazioni tabellari di cui uno è Cosmos, che tiene traccia di tutti gli eventi passati.

I seguenti principi architettonici hanno guidato le decisioni di progettazione della piattaforma AEP, come descritto qui.

- Ogni funzionalità principale è implementata come microservizio.
- Ogni microservizio è versionato in modo indipendente dagli altri prodotti.
- La topologia dell'API è coerente tra i microservizi, unificando la semantica dell'API e le implementazioni tecniche.
- Tutti gli scenari realizzabili attraverso i client (app, sito web) sono realizzabili anche attraverso una sequenza di chiamate API grezze.

3.2.3. Natural Language Processing e Text Mining per individuare l'impatto sui profili professionali delle tecnologie e delle innovazioni tecnologiche

Nel dibattito su quali siano le chiavi per interpretare l'effettivo impatto delle innovazioni tecnologiche e della digitalizzazione dei processi di lavoro, come anche dei metodi di lavoro, sulla resilienza di mestieri, job e competenze, interviene a supporto decisivo l'applicazione del Natural Language Processing.

Infatti, poter effettuare ed avere evidenza delle correlazioni e delle co-occorrenze tra il trend di una tecnologia specifica e una competenza ovvero un cluster di competenze che caratterizzano una professione, un ruolo, una mansione, porta a programmare un ciclo o trend di obsolescenza della mansione oggetto di indagine.

Evidentemente è un metodo per concretamente sfatare oppure dare forma all'esito del dibattito su quale impatto può avere una tecnologia rispetto alla sopravvivenza di mansioni intesi come posti di lavoro, in termini di parziale o completa sostituzione, così come di supporto in termini di concorrenza positiva ed evoluzione di una professionalità, o così come di una neutralità (mancanza di impatto) dell'effetto di un'hype tecnologica rispetto ad un set di competenze.

Il ruolo giocato da algoritmi di NLP è decisivo per una possibilità, ad oggi, tecnicamente irraggiungibile diversamente: indagare, collettare, confrontare, correlare e connettere informazioni e dati presenti in testi scritti in linguaggio naturale. E, da queste analisi, far emergere trend complessi.

Per "testi" intendiamo: letteratura tecnico-scientifica (paper, abstract, articoli, manuali, ecc.), testi normativi e regolamentativi, atlanti delle professioni e delle competenze, repertori di qualifiche nazionali o regionali o di altre autorità, repertori di brevetti registrati e in via di registrazione, previsioni di andamenti del mercato del lavoro, previsioni e tendenze nelle evoluzioni tecnologiche, fonti web accreditate e non. In termini quantitativi, benchè di per sé poco significativo come dato, parliamo di milioni di "pagine" e fonti dato testuali.

Questo primo contenitore di testi, configurabile (selezionabile, estendibile o restringibile) a seconda degli obiettivi particolari dell'analisi, si confronta con i job title e le job description che vogliamo mettere al centro dell'attenzione: del

decisore HR (pubblico o privato che sia), del policy maker, del CIO, del COO, dell'R&D, del CTO, dell'associazione di categoria/settore/rappresentanza, del sindacato, albo/ordine professionale, ecc.

Dunque, algoritmi, brevetti o combinazione di brevetti basati su NLP possono compiere queste operazioni, sia che siano scritti (programmati) ad hoc di volta in volta sia che siano embedded in piattaforme o veri e propri tool dedicati.

In termini di applicazioni concrete che possiamo citare all'interno di questo use case ne abbiamo almeno 3 che rispondono ad esigenze simili tra loro e le segnaliamo in forma di domanda, di quesito generativo, così come si presenta effettivamente nel mercato:

- (Decisore Pubblico): Come posso confrontare la mia offerta di mestieri pubblici, caratterizzata da certi metodi di lavoro, competenze, set di tecnologie che devono essere note ed usabili, con il mercato del lavoro privato? Come posso affrontare la scarcity attingendo al bacino di potenziali lavoratori che guardano con meno interesse al mondo pubblico rispetto al privato? Quali competenze correlate a tecnologie di analoghi mestieri del Privato posso integrare al mio repertorio di mansioni e competenze Pubblico (pensando ad un ente locale o ad una amministrazione centrale dello Stato, per esempio, o ad una sua diramazione territoriale o agenzia)?
- (Decisore Privato – Azienda): Quali innovazioni tecnologiche devo incorporare in quali processi di lavoro o in quali professionalità dell'ampio settore del farmaceutico-scienze della vita-biotecnologie? Quali investimenti su quali macchine devo commisurare rispetto alla dotazione di competenze tecniche attuale e futura?
- PNRR: che tipo di mercato del lavoro e delle competenze determina l'applicazione del Piano a seconda che il Piano stesso sostenga lo sviluppo della Sostenibilità (Green New Deal) e/o le trasformazioni digitali?

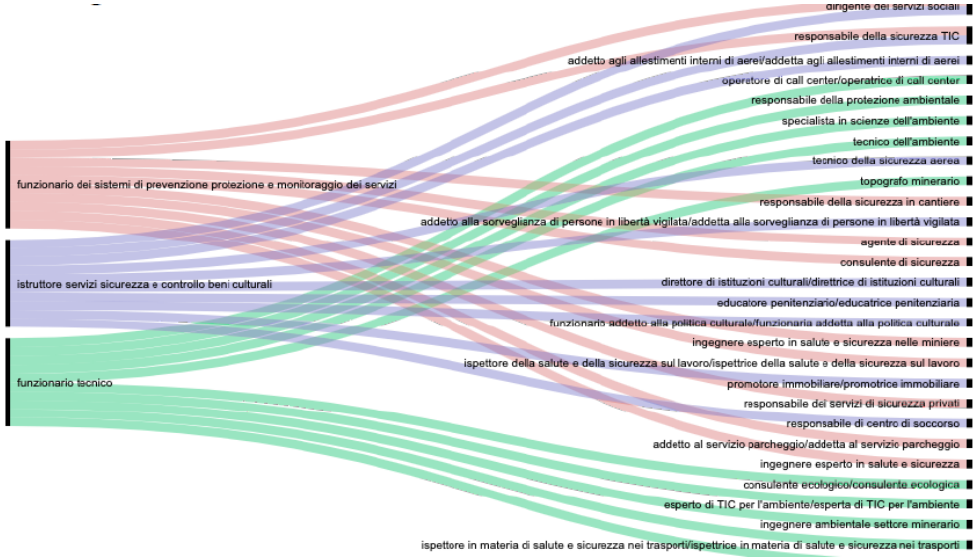
Caso del Decisore pubblico

Ci troviamo dentro un grande comune del Centro-Italia che deve porre mano a strumenti di programmazione del Personale per via della introduzione di "Quota 100".

L'occasione è utile per rivedere le competenze dichiarate nelle declaratorie del mansionario in logica di previsione di prossime future assunzioni massive, così che i potenziali candidati riconoscano, nelle posizioni offerte, competenze presenti anche nel mondo del privato e sia facilitata la traduzione da entrambi i mercati del lavoro.

Gli algoritmi di Natural Language Processing portano a comparare quali professioni private possano riversare nelle equivalenti o similari professioni pubbliche delle competenze di interesse per l'ufficio ricevente.

Nelle successive due immagini si trovano – per esemplificare - visualizzazioni di quali profili professionali del Privato (a destra) siano riconducibili, per determinate competenze, a determinate professioni dell'ente committente (a sinistra).



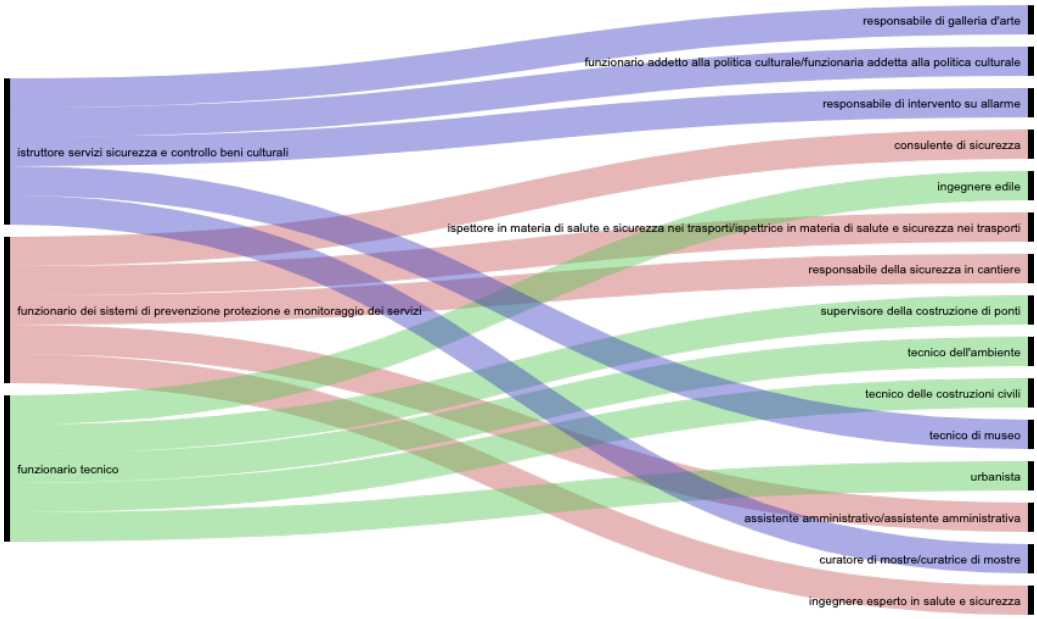


Figure 20a e 20b. Corrispondenze tra professioni nel settore privato (dx) e nel settore pubblico (sx)

Il bacino del mercato del lavoro così individuato diventa terreno di coltura per politiche di attraction e di comunicazione per l'ente committente.

Caso del Decisore Privato

Ci troviamo nel Dipartimento HR di una grande azienda del farmaceutico. L'azienda deve allineare ad uno standard di competenze più stabilimenti produttivi, ma lo deve fare tenendo conto di quali possano essere i prossimi investimenti in tecnologie da parte dell'azienda, su tutti gli stabilimenti in questione.

Il Dipartimento HR comprende che se venissero fatti degli investimenti senza comprendere la ricaduta sui mansionari dei dipendenti maggiormente impattati, la finalità di breve-medio periodo degli stessi investimenti sarebbe a priori messa in discussione. Pertanto decide di applicare il NLP a mansionari, brevetti e brevetti in via di registrazione, letteratura tecnico-scientifica di settore (field in cui opera l'impresa), repertori internazionali di mansioni, repertori di tecnologie di interesse per gli investimenti del Gruppo. Ne derivano una serie di mappe e

di assumptions utili alla rilevazione di alcune variabili chiave di seguito esemplificate in immagine.

La readiness digitale fotografata relativa ai profili professionali si è estesa quindi a metodi di lavoro oltre che alle competenze, generando una mappa (linee guida, propedeuticità) per il Dipartimento committente che guida la possibile trasformazione tecnologica a partire dalle persone.

Figura 21. Schema di assessment della readiness digitale. Fonte: Mylia.

Caso del rapporto tra PNRR e Mercato del lavoro

All'indomani della pubblicazione del PNRR italiano da parte del Governo, immediata è stata la reazione di molti operatori del mercato del lavoro (agenzie per il lavoro, istituti di statistica, associazioni di categoria, enti di formazione, ecc.) per capire le traiettorie di impatto.

Utilizzando tecniche di NLP si è potuto rilevare un chiaro percorso privilegiato per alcune professionalità caratterizzate da specifici repertori di skills, sia seguendo la traiettoria dettata dagli investimenti sul Green sia seguendo quella relativa agli investimenti sul Digital.

Ciò è stato possibile perché gli algoritmi hanno aggredito le analisi del Bureau Of Labour degli USA, tenute a benchmark di alcuni sviluppi tecnologici in

correlazione green&digital, e le hanno correlate a loro volta a specifiche tecnologie (talune più interessanti in ambito Green, talaltre in ambito 4.0) di interesse per il nostro Paese nella lettura del PNRR.

L'analisi è stata condotta utilizzando O*NET (Occupational Information Network) come fonte primaria di dato, poiché direttamente connessa alle statistiche di Bureau e da cui è possibile desumere le professionalità più richieste in ottica previsionale (definite "bright outlook"), le tecnologie più richieste nel job posting (definite "hot technologies") e i profili nati per gestire l'impatto delle attività della green economy (definite "green occupations").

Le occupazioni Bright Outlook, in particolare, sono di estremo valore strategico poiché si prevede che cresceranno rapidamente nei prossimi 10 anni a livello di richiesta di mercato.

Gli output che ne sono derivati sono stati i seguenti:

- Lista di profili emergenti e di successo per il Digital (circa una cinquantina)
- Lista di profili emergenti e di successo per il Green (circa venti)

entrambe con l'elenco delle competenze chiave in ranking prioritario.

Le skills di maggior interesse per i due settori ed in comune tra i due sono sotto rappresentate in tabella.

Le skill digitali fondamentali per i futuri professionisti dei settori green e digital

Adobe System Adobe Acrobat	●	●	ESRI ArcView 3D Analyst	●	○
Adobe System Adobe Illustrator	●	●	Extensible markup language XML	●	●
Adobe System Adobe InDesign	●	●	Geographic information system GIS software	●	●
Adobe System Adobe Photoshop	●	●	Go	○	●
Advanced business application programming ABAP	○	●	Google Analytics	●	●
AJAX	○	●	IBM SPSS Statistics	●	●
Amazon Dynamo DB	○	●	JavaScript	●	●
Amazon Elastic Compute Cloud EC2	○	●	Linux	●	●
Amazon Redshift	○	●	Minitab	●	●
Amazon Web Services AWS software	○	●	MySQL	●	●
Apache Ant	○	●	Oracle Java	○	●
Apache Cassandra	○	●	Oracle software	●	●
Apache Groovy	○	●	Practical extraction and reporting language Perl	●	●
Apache Hadoop	○	●	Python	●	●
Apache Hive	○	●	R	●	●
Apache HTTP Server	○	●	Relational database management software	○	●
Apache Kafka	○	●	Salesforce software	●	●
Apache Pig	○	●	SAP Crystal Reports	○	●
Autodesk AutoCAD	●	○	SAP software	●	○
Autodesk AutoCAD Civil 3D	●	○	SAS	●	●
Autodesk Revit	●	○	Social media sites	●	●
Bentley MicroStation	●	○	Structured query language SQL	●	●
C#	○	○	Tableau	●	●
C++	●	●	Teradata Database	○	●
Computer aided design CAD software	●	○	The MathWorks MATLAB	●	●
ESRI ArcGIS software	●	●	UNIX	●	●

● Green ● Digital ●● In comune

Figura 22. Tabella delle digital e green skills fondamentali. Fonte: Mylia.

3.3. Digital Twin per smart asset e facility management (Exprivia)

Il caso di utilizzo del Digital Twin in fase di Operation&Maintenance descrive una strategia di gestione intelligente di un asset rispetto alle strategie di gestione tradizionali.

Il gemello digitale rappresenta una copia esatta dell'asset fisico e, a seguito della raccolta ed elaborazione dei dati provenienti dalle diverse sorgenti dati, diventa la cosiddetta "single source of truth", cioè l'unico contenitore in grado di fornire tutte le informazioni sul comportamento reale dell'opera.

Il Digital Twin può alimentare algoritmi di IA al fine di migliorare le performance dell'asset che rappresenta, ma anche per migliorare le performance di qualsiasi asset con le stesse caratteristiche. Si parla di Smart asset e facility management perché l'asset diventa intelligente grazie ai feedback provenienti dal gemello digitale e lavora in maniera autonoma sulle proprie performance.

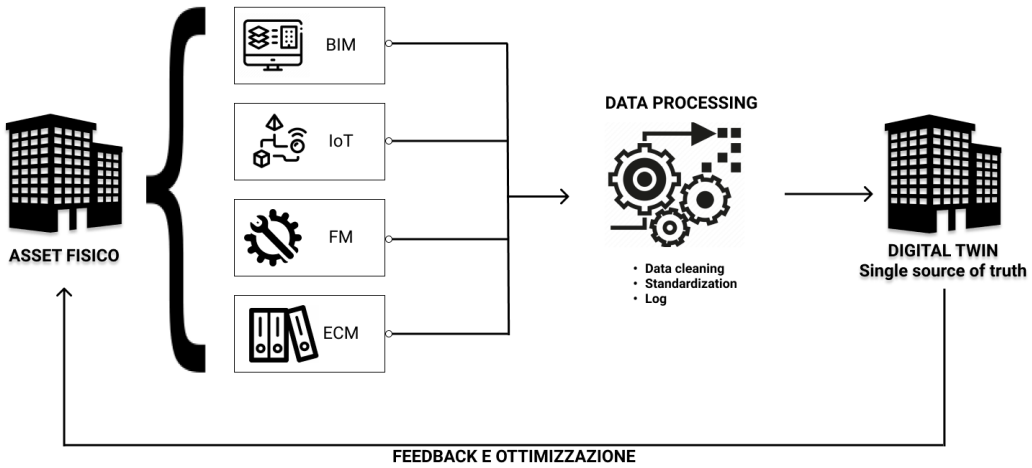


Figura 23. Schema rapporto asset fisico – DT. Fonte: Exprivia.

Alcune applicazioni di strategie di gestione smart delle attività di operazione e manutenzione sono:

- Ottimizzazione dei consumi energetici, sia dal punto di vista termico che illuminotecnico, tramite elaborazione dei dati provenienti da BMS (Building Management Systems) per rilevare ad esempio le fasce orarie in cui gli impianti possono lavorare in maniera ridotta poiché gli spazi sono occupati differentemente da quanto previsto nella fase di progettazione
- Manutenzione preventiva tramite monitoraggio anomalie: nel momento in cui vengono riscontrati dei comportamenti anomali negli impianti o nelle strutture, il modello digitale può mostrare un allarme ed individuare delle strategie per ridurre le conseguenze dell'anomalia riscontrata, ad esempio sostituzione dell'oggetto da cui arriva la segnalazione prima che arrivi a rottura
- Manutenzione predittiva tramite analisi dati storici, il cui obiettivo è quello di definire un piano di manutenzione dell'asset che metta in relazione i dati storici raccolti sia dall'asset oggetto di manutenzione che da asset simile, ma anche da quanto previsto in fase di progettazione. Questo consente di prevedere gli interventi di manutenzione ordinaria e straordinaria elaborando eventualmente scenari alternativi tra loro per individuare un bilancio tra risorse e performance.

3.4. Use case di Generative AI (Engineering)

3.4.1. Generative AI per l'elaborazione dei volti

Negli ultimi anni, la generative AI ha fatto enormi passi nel campo delle immagini in generale e, più nello specifico, nella generazione di volti; grazie alle più recenti tecnologie di Deep Learning infatti, la comunità scientifica ha sviluppato modelli matematici sempre più avanzati in grado di apprendere dai dati di input e di generare volti del tutto paragonabili a quelli reali, indistinguibili.

Un ruolo importante in tal senso è ricoperto dalle Generative Adversarial Networks (GANs): reti neurali artificiali utilizzate nell'apprendimento automatico, tipicamente per generare immagini, suoni e altri dati sintetici. Le GAN utilizzano due reti neurali: un generatore che crea campioni e un discriminatore che valuta la qualità di tali campioni. Il generatore cerca di creare campioni che possano ingannare il discriminatore, mentre il discriminatore cerca di distinguere i campioni reali da quelli generati dal generatore. Le GAN sono state inoltre utilizzate in diversi campi, oltre alla generazione di immagini, come ad esempio la sintesi di voce e la creazione di dati sintetici strutturati e non strutturati. Altri sistemi di rilievo sono i Variational Autoencoders (VAEs): una classe di reti neurali artificiali utilizzate nell'apprendimento automatico e nella generazione di dati piuttosto generali. Sono un tipo di autoencoder probabilistico che utilizza tecniche di inferenza bayesiana per apprendere una rappresentazione latente dei dati di input. Sono composti da due parti: il "codificatore" e il "decodificatore".

I VAE sono stati utilizzati in diverse applicazioni, come la generazione di immagini, la compressione di dati e l'analisi di dati di serie temporali. Questi modelli hanno importanti applicazioni in ambito creativo, artistico e commerciale, come la generazione di foto di volti estremamente fotorealistici a partire da una descrizione testuale nel momento in cui si effettua l'identikit di un soggetto o la creazione di avatar di chatbot quasi indistinguibili da persone reali.

Una delle architetture modellistiche più note per la generazione di volti, basato sull'architettura GANs, è chiamata StyleGAN (Style-based Generative Adversarial Network), sviluppato da NVIDIA. Mentre modelli come le StyleGAN sono utili per la generazione di un immagine, esistono modelli probabilistici

basati sulla tecnica del "continuous flow" che sono utili a controllare il contenuto della generazione; questi possono permettere ad esempio il controllo di attributi estremamente di dettaglio all'interno di un volto come la presenza o meno di lentiggini, o la curvatura delle sopracciglia.

3.4.2. Generative AI per conversazioni su dominio specializzato

La storia della generative AI in ambito conversazionale pone le sue radici nel campo del Machine Learning e della modellizzazione probabilistica; questa esiste in realtà da diversi anni, probabilmente da quando ELIZA, un chatbot che simula la conversazione con un terapeuta, è stato sviluppato dal MIT nel 1966. Nei primi anni 2000, la generative AI iniziò a ricevere maggiore attenzione grazie alla diffusione di algoritmi di Deep Learning e in generale delle Artificial Neural Network; questi algoritmi hanno permesso di creare modelli matematici complessi in grado di apprendere dai dati di input e di generare, di conseguenza, informazioni in modo autonomo con un elevato grado di affidabilità. Sono ora maturi i tempi per avere un sistema artificiale in grado di comprendere il linguaggio naturale di un umano e di sviluppare con esso un ragionamento, esponendolo a sua volta in linguaggio naturale attraverso un avatar che si muove in sincronia e con la voce.

Per generare una conversazione sono utilizzabili diverse sistemi analitici complessi, eventualmente anche combinati tra loro; una delle architetture modellistiche più utilizzate in questo momento storico sono i transformers: un tipo di architettura di rete neurale artificiale utilizzata nell'apprendimento automatico, in particolare nell'elaborazione del linguaggio naturale. Sono stati introdotti per la prima volta nel 2017 in un paper intitolato "Attention is All You Need" e da allora sono diventati una delle architetture più utilizzate nel campo del NLP. I Transformers utilizzano l'attenzione per elaborare sequenze di input e output. Questo significa che le reti neurali non elaborano i dati in modo sequenziale, ma piuttosto considerano l'intera sequenza contemporaneamente. Ciò consente ai Transformers di ottenere risultati migliori rispetto alle architetture precedenti, come le Reti Neurali Ricorrenti. Facendo riferimento alle tecnologie, nello specifico, relativamente alla tecnologia dei Transformers, la tipologia di modelli detti Large Language Models (LLMs), ovvero modelli di linguaggio con un elevato numero di parametri ha visto una fortissima crescita negli ultimi anni.

Un LLM è un tipo di modello di Intelligenza artificiale che utilizza reti neurali per analizzare grandi quantità di testo e generare output che hanno senso dal punto di vista semantico e sintattico. Questi modelli sono addestrati su enormi quantità di dati, spesso miliardi di parole, attraverso l'utilizzo di algoritmi di deep learning. Sono in grado di creare una "rappresentazione interna" del linguaggio naturale, permettendo al modello di capire il contesto in cui le parole sono utilizzate. Grazie alla loro capacità di comprendere il contesto e di generare testo in modo autonomo, i modelli LLM sono utilizzati in una vasta gamma di applicazioni di elaborazione del linguaggio naturale, tra cui la traduzione automatica, la generazione di testo, la risposta alle domande e molto altro ancora.

Uno dei più grandi LLM attualmente disponibili è GPT-3 (Generative Pre-trained Transformer 3), sviluppato da OpenAI, che contiene 175 miliardi di parametri e può generare testo con una qualità sorprendentemente alta. Utilizza una combinazione di tecniche di deep learning, tra cui le reti neurali a trasformatori (Transformer Neural Networks), per generare testo in modo autonomo. GPT-3 è stato addestrato su una vasta quantità di dati, compresi testi di libri, articoli di giornale, pagine web e molto altro ancora. Una delle caratteristiche più sorprendenti di GPT-3 è la sua capacità di generare testo che sembra essere stato scritto da un essere umano. Questo modello è in grado di creare frasi e paragrafi coerenti e ben strutturati e può imitare lo stile di scrittura di un determinato autore o di un determinato genere di testo. Una delle implementazioni più note di GPT-3 è nota come ChatGPT.

L'impiego di queste tipologie di modelli conversazionali può avvalersi di alcune strategie per assicurare una risposta il più accurata possibile, tra le quali, in particolare: la costruzione e l'uso di prompt e il fine tuning. L'utilizzo dei prompt è un'importante strategia per migliorare la qualità e la accuratezza dei risultati generati dagli LLM. Fornendo al modello un contesto specifico e chiaramente definito, è possibile ottenere output più pertinenti e rilevanti. Supportare l'utilizzo dei prompt con un sistema di information retrieval accentua ulteriormente l'accuratezza delle risposte fornite all'utente. Quando l'utilizzo del prompt non permette il raggiungimento dell'accuratezza si può ricorrere alla fase di fine tuning, addestrando il modello sul dominio specifico da trattare, in modo da coprire le peculiari esigenze di impiego a cui dovrà il modello dovrà essere rivolto.

L'interazione, a livello più semplice vede l'adozione di soluzioni "speech to text" e "text to speech" per cui il dialogo tra l'utente e il chatbot può avvenire in forma del tutto naturale in modo che l'utente esponga a voce la richiesta e la risposta ritornata dal chatbot a sua volta sarà espressa nella stessa forma.

3.5. Assistenti virtuali nel contest di una grande amministrazione centrale (DXC)

L'utilizzo degli assistenti virtuali all'interno di una grande pubblica amministrazione centrale consente di disporre di una piattaforma di assistenza di primo livello che porta:

- alla riduzione progressiva delle richieste di Assistenza per i diversi procedimenti amministrativi;
- alla presenza di un supporto 7/7gg h24;
- alla semplificazione nella divulgazione dei contenuti informativi aziendali (FAQ, Documentazione ufficiale);
- al miglioramento del servizio attraverso la raccolta di statistiche di utilizzo e feedback utenti;
- alla mitigazione del rischio di contenziosi su processi critici passando per una comunicazione più chiara ed efficace;
- all'indirizzamento contestualizzato delle richieste non gestite, verso livelli di assistenza superiori.

Lo sviluppo degli Assistenti Virtuali parte da un'approfondita conoscenza del dominio applicativo. Infatti partendo da una Knowledge base strutturata ed organica, è possibile procedere alla costruzione e successivo addestramento di un modello cognitivo di Natural Language Processing, a supporto dell'Assistente, che gli consente di interpretare correttamente le richieste utente.

L'addestramento rappresenta un processo iterativo, che passa attraverso numerosi test atti a simulare l'esperienza utente, con la finalità di raccogliere evidenze utili a comprendere il funzionamento del modello cognitivo ed identificare eventuali aree di miglioramento.

In una logica di semplificazione delle attività di distribuzione e di miglioramento continuo del servizio, inoltre, i modelli cognitivi devono essere sviluppati, versionati, distribuiti e monitorati secondo le pratiche dell'MLOps, le cui caratteristiche e benefici sono stati ampiamenti discussi all'interno del paragrafo 1.5 del presente documento.

Per lo sviluppo degli assistenti virtuali è stato utilizzato un framework modulare, incentrato sui seguenti pillar:

- Dati: sorgenti da cui reperire info utili allo sviluppo della Base di Conoscenza (DB strutturati o non strutturati, Pagine web, Documenti digitali ecc.) sottostante al modello di Intelligenza artificiale;
- Funzioni abilitanti: si tratta delle features caratterizzanti per ciascun caso d'uso. Possono essere agganciate in modalità "plug&play", oppure sviluppate ad hoc, in base alle esigenze. Si riporta di seguito una lista sintetica delle principali funzionalità disponibili all'interno del framework:
    - *INTERAZIONE VOCALE* Permette di rendere fluida e naturale la conversazione con l'assistente attraverso il semplice utilizzo della voce.
    - **INTERROGAZIONE SU BASE DATI** Permette di generare, in maniera dinamica, delle query da sottoporre alla Base Dati, direttamente a partire da richieste utente espresse in linguaggio naturale.
    - **RICERCA SEMANTICA SU BASE DOCUMENTALE** Consente all'utente, quando formula una richiesta in linguaggio naturale, di ottenere una risposta che riporti le informazioni estrapolate da alcuni documenti ufficiali.
    - **SUPPORTO TELEFONICO** Possibilità di ricevere un supporto sempre attivo (24/7), direttamente su canale telefonico, a cui risponde un assistente virtuale, in grado di comprendere le richieste utente in linguaggio naturale e fornire la risposta più appropriata rispetto all'informazione ricercata, attinente ad un certo contesto applicativo.
    - **SUPPORTO DI LIVELLO SUPERIORE In tutti quei casi per cui l'utente avesse necessità di ricevere un supporto**

dedicato, potrà sempre attivare un flussi di supporto avanzato (apertura ticekt, inoltro all'operatore umano, ecc)

- Analytics layer: i log conversazionali, unitamente a feedback puntuali richiesti agli utenti per validare la correttezza e la completezza del supporto fornito a fronte di ciascuna richiesta, concorrono ad alimentare una piattaforma di Data Analytics da cui estrarre insights utili a monitorare l'utilizzo dell'Assistente ed individuare possibili aree di miglioramento.

Segue una panoramica d'insieme del framework discusso:

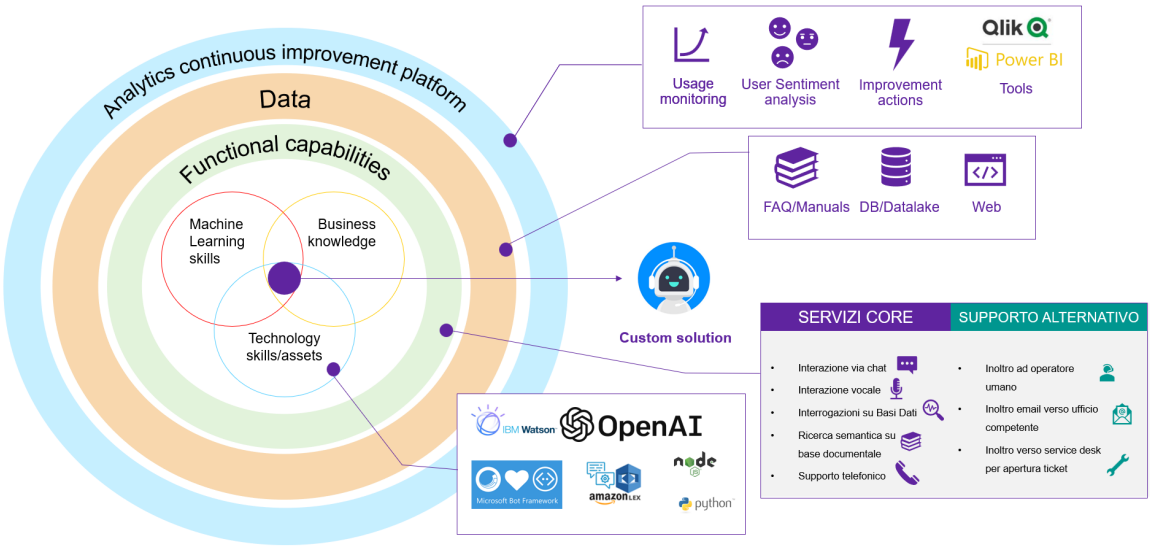


Fig. 24 Framework per lo sviluppo di assistenti virutali. Fonte: DXC

Nell'ambito di una grande amministrazione centrale sono stati realizzati assistenti virtuali accessibili dall'area pubblica e privata del sistema informativo dell'amministrazione centrale con l'obiettivo di fornire supporto a classi di utenza differenti.

Gli assistenti virtuali realizzati nell'area pubblica operano sia su contesti generali sia su contesti specifici e sono rivolti prevalentemente alla cittadinanza con un ampio bacino di utenza.

Lo strumento è stato integrato sul portale istituzionale dell'URP (Ufficio Relazioni con il Pubblico) e sul canale ufficiale Facebook Messenger dell'Amministrazione e offre risposte su temi amministrativi di carattere generali contestualizzate sulla tipologia di utenza che viene identificata nel corso della conversazione.

Gli assistenti virtuali presenti nell'area privata sono invece a supporto di specifiche classi di utenza appartenenti all'amministrazione e sono addestrati su specifici procedimenti amministrativi. I contenuti presentati all'utente sono arricchiti con collegamenti ipertestuali (link) ed immagini. La conversazione con l'assistente virtuale può essere condotta sotto forma di chat testuale oppure attraverso l'impiego della voce. Oltre alla consultazione di contenuti informativi standard, all'utente viene offerta anche la possibilità di estrarre informazioni puntuali rispetto al proprio personale contesto attraverso delle query su DB eseguite a fronte di richieste in linguaggio naturale. La chatbot restituisce quindi risposte personalizzate rispetto alla propria posizione nell'esecuzione dei procedimenti amministrativi.

Le chatbot fanno inoltre parte di un modello integrato di assistenza, per cui nel caso l'utente non trovi soddisfacente la risposta fornita, gli verrà inoltre offerta la possibilità di

- Aprire un tagliando verso Service Desk Online (supporto specialistico di secondo livello) per approfondimenti di natura amministrativa e tecnica;
- Contattare il numero verde del Sistema Informativo per supporto di tipo applicativo;
- Attivare una ricerca semantica su una base di conoscenza di tipo documentale (manuale utente, focus su temi specifici, checklist operative ecc.) al fine di estrarre i contenuti più attinenti alla richiesta utente, con l'utilizzo dell'AI.

3.6. Dati Sintetici per software testing (AINDO)

Effettuare il software testing con dati di prova accuratamente rappresentativi è essenziale per fornire soluzioni IT all'avanguardia. Purtroppo, per testare nuovi prodotti IT sono necessarie grandi quantità di dati. Di solito, i dati reali non possono essere utilizzati per i test a causa delle restrizioni sulla privacy. I dati di prova vengono quindi creati manualmente, attraverso processi macchinosi.

Ciò richiede un notevole dispendio di denaro, tempo e personale. Spesso può anche essere necessaria una consulenza esterna per assicurarsi che i dati di prova siano sufficientemente accurati. Inoltre, i cambiamenti che avvengono durante il processo di sviluppo del software possono man mano rendere necessari formati, strutture o attributi dei dati diversi.

I dati sintetici replicano i dati reali senza contenere informazioni sensibili. Pertanto, la loro qualità è superiore a quella dei dati di prova costruiti manualmente. Inoltre, i dati sintetici sono immediatamente disponibili e flessibili: se i requisiti cambiano durante il processo di software development, i dati sintetici possono essere aggiornati direttamente per riflettere le nuove esigenze. I dati sintetici possono anche essere riequilibrati per modellare determinate rarità e anomalie. Questo aiuta a verificare che il software funzioni con affidabilità anche in presenza di anomalie ed eventi inaspettati.

La tecnologia dei dati sintetici può essere applicata a vari casi di software testing, come ad esempio nel caso di un produttore di dispositivi medici che deve sviluppare un software per dei pacemaker. Il pacemaker è un dispositivo elettronico che viene impiantato chirurgicamente all'interno del corpo, in genere sotto la clavicola, e viene utilizzato per trattare le aritmie cardiache. Invia impulsi elettrici per stimolare i muscoli del cuore e regolare le sue contrazioni per produrre il battito cardiaco. Il software del pacemaker monitora continuamente l'ampiezza dei battiti cardiaci e il tempo che intercorre tra un battito e l'altro. Il software utilizza questi dati per determinare se è necessario un impulso elettrico artificiale in qualsiasi momento.

Gli algoritmi del pacemaker devono essere estremamente robusti in risposta alle anomalie: il dispositivo deve essere in grado di agire con accuratezza anche quando vengono registrate attività cardiache inaspettate, per esempio un battito anomalo (più lento o più veloce del solito). L'algoritmo decisionale utilizzato deve essere anche altamente efficiente ("minimal") per diversi motivi: innanzitutto, i pacemaker sono molto piccoli e quindi hanno una potenza di calcolo limitata; in secondo luogo, le decisioni del software devono avvenire rapidamente, nell'ordine di nanosecondi; infine, gli algoritmi semplici consentono una maggiore durata della batteria, limitando così il numero di escissioni e di re-impianti del dispositivo nel paziente.

La tecnologia dei dati sintetici può facilitare dunque il test e l'ottimizzazione di nuovi software per i pacemaker per diversi motivi. Innanzitutto, non è necessario disporre di dati reali dei pazienti; si possono evitare perciò le fasi di

elaborazione intensiva dei dati in conformità ai protocolli sulla privacy. Perdipiù, non è necessario sviluppare manualmente i dati di prova. Inoltre, i dati sintetici possono offrire la possibilità di aumentare artificialmente il numero di anomalie attraverso la data augmentation. Quest'ultima permetterebbe infatti di colmare le lacune esistenti nel set di dati per quanto riguarda le anomalie, rafforzando la robustezza del software. In questo modo, grazie ai dati sintetici, non solo si potrebbero ridurre sostanzialmente i costi e i tempi di sviluppo, ma si potrebbe anche migliorare in modo significativo l'affidabilità del prodotto.

4. PARTE QUARTA – SCENARI DI APPLICAZIONE SU VERTICALI

Si considerano alcuni settori verticali delineando i potenziali impatti portati dalla applicazione della IA evidenziando difficoltà e opportunità che i vari player dovranno affrontare.

4.1. Cybersecurity (Leonardo)

L'ultimo rapporto CLUSIT descrive non solo un aumento dell'+8,3% nel numero di attacchi rispetto allo stesso periodo del 2021, ma indica come il 22% degli attacchi sia stato realizzato con algoritmi complessi, ovvero con codice sofisticato.

Le tecniche degli hacker si raffinano continuamente e i malware messi in circolazione, da generici, diventano sempre più sofisticati e mirati con precise finalità distruttive e/o estorsive.

In molti casi si tratta di attacchi effettuati da hacker sponsorizzati (da Stati o aziende) che hanno un target specifico (spionaggio industriale, frodi, terrorismo, …) e che possono contare su una rete di risorse e capacità, messe in condivisione anche in modalità "as a service".

L'uso di tecniche di Intelligenza artificiale e di machine learning facilita la ricerca della migliore vulnerabilità, individuando i migliori target da colpire (anche in ambienti OT) e i comandi più corretti per danneggiarli.

Dal punto di vista dell'attaccante, l'attacco può essere suddiviso in white-box (se l'attaccante ha una conoscenza completa del model target) e black-box (se l'attaccante non conosce l'architettura della rete neurale, i parametri e altre informazioni sul modello).

Spesso l'intruso che ha fatto breccia all'interno di un'infrastruttura rimane silente all'interno della realtà da colpire e si muove indisturbato per raccogliere informazioni e individuare il punto di debolezza migliore.

L'Intelligenza artificiale viene inoltre utilizzata dagli hacker per effettuare attacchi più rapidi su più obiettivi contemporaneamente.

L'IA viene utilizzata per generare diversi tipi di attacchi:

- Uno dei principali modi in cui gli attaccanti utilizzano l'IA è tramite l'elaborazione del linguaggio naturale (NLP) che consente ai criminali di creare messaggi di phishing che sembrano provenire da fonti affidabili.
- Un altro modo in cui l'IA viene utilizzata dagli attaccanti è tramite l'apprendimento automatico. Gli attaccanti possono utilizzare l'apprendimento automatico per analizzare grandi quantità di dati e individuare vulnerabilità nei sistemi informatici.
- Inoltre, l'IA viene utilizzata dagli attaccanti per creare malware, ultimamente anche utilizzando la code generation di strumenti come chatgpt, che è in grado di adattarsi e modificare il proprio comportamento in tempo reale. Questo rende il malware molto più difficile da individuare e da combattere.
- Infine, l'IA viene utilizzata anche per attacchi di tipo "brute force", generando molteplici combinazioni di password e di altre informazioni di accesso al fine di individuare la combinazione corretta.

Se questo è lo scenario di riferimento, è chiaro che la difesa cyber deve poter contare su capacità altrettanto evolute.

Già da alcuni anni, l'IA è utilizza per anticipare il rilevamento di una minaccia sfruttando la tecnologia per elaborare e correlare un'ingente mole di informazioni alla scoperta di malware già noti o anche di comportamenti anomali, di per sé legittimi e non dannosi, ma che si rivelano segnali deboli che qualcosa di strano sta avvenendo.

Tali tecniche si basano sull'analisi di tutte le informazioni sull'utilizzo delle reti, applicazioni e dati a disposizione per definire dei pattern da confrontare con una base di riferimento di normalità. L'IA, inoltre, può adattarsi alle minacce informatiche in evoluzione e imparare dai modelli di comportamento delle minacce stesse, rendendone la gestione più efficiente e dinamica.

In questo modo è possibile portare all'attenzione una situazione potenzialmente dannosa (non una signature già codificata) e avviare un'azione immediata di verifica.

In questo contesto, l'IA non va intesa come capacità realmente autonoma, ma a supporto di analisti esperti, portando all'attenzione correlazioni tra eventi che altrimenti sfuggirebbero alle capacità umane:

- L'IA può automatizzare gran parte delle attività ripetitive nella gestione della sicurezza informatica, consentendo ai team di sicurezza di concentrarsi su

attività più avanzate e complesse e può aumentare l'efficienza dei processi di gestione della sicurezza informatica, consentendo ai team di rispondere alle minacce in modo più rapido ed efficace.

- L'AI può ridurre il rischio di errori umani nella gestione della sicurezza informatica, aumentando l'accuratezza e l'affidabilità delle attività di sicurezza.
- L'AI, nelle sue applicazioni di Machine Learning e Deep Learning, consente l'apprendimento dei fenomeni e dei comportamenti e la loro visualizzazione in un formato leggibile all'analista in modo da rilevare le attività anomale e poter così anticipare le mosse dell'attaccante.

Nel corso del tempo, sono state introdotte funzionalità AI più avanzate, come per esempio l'integrazione di fonti esterne di dati provenienti da sistemi di sicurezza diversi, acquisendo un quadro sintetico ed esaustivo, più facilmente analizzabile, in modo da poter prendere più facilmente decisioni.

Ha trovato inoltre sempre più impiego nell'analizzare i rischi connessi ad un attacco in relazione alla criticità di un sistema e nel prioritizzare, anche sulla base della conoscenza sulle minacce proveniente dalla threat intelligence.

Inoltre l'Intelligenza artificiale incentrata sulla sicurezza permette di supportare l'individuazione delle azioni di contenimento che si sono rivelate efficaci in quel contesto, oltre a consentire di coordinare le operazioni contro il malware e di agire più rapidamente tramite processi di automazione.

L'elemento umano rimane la parte più pregiata sia nella fase di investigazione che nella gestione dell'incidente, dal momento che le tecniche di attacco cambiano continuamente e non si basano su schemi fissi, ma le tecnologie posso potenziare enormemente le capacità di difesa.

È importante sottolineare che l'uso della IA è tanto più efficace quanto più è alta la qualità e la quantità dei dati presi in esame.

È indispensabile avere un punto unificato dove vengono rilevati i comportamenti di tutte le componenti (sistemi, rete, applicazioni e dati) in modo che gli strumenti di Intelligenza artificiale possano immediatamente identificare le tipologie di attacco, valutare i servizi potenzialmente impattati e scegliere le strategie di reazione e contenimento più adatte.

4.2. Legal Technology (Eustema)

Nel settore delle tecnologie per l'ambito legale (denominato Legal Tech) l'Intelligenza artificiale al servizio delle strutture legali delle avvocature e dei grandi studi legali ha lo scopo di:

- Semplificare le attività durante la gestione delle pratiche legali e supportare le scelte operative degli utenti (**Aumento della produttività**);
- Guidare le scelte per una più efficace gestione dei processi all'interno della struttura legale (**Supporto alle decisioni strategiche**)
- Supportare i processi aziendali esterni alla struttura legale, contribuendo a individuare punti di miglioramento, possibili azioni correttive e rischi/benefici annessi (**Valore all'Organizzazione**);

Le applicazioni di Legal AI abbracciano tre direttrici:

- **Legal Automation:** applicazioni in grado di automatizzare una serie di attività svolte dai professionisti dell'area legale durante la gestione della pratica;
- **Legal Discovery:** applicazioni in grado di offrire un'esperienza avanzata di ricerca intelligente su documenti e contenuti non strutturati e ricercare per concetti, entità, parole semanticamente simili, citazioni, riferimenti legislativi, ecc.
- **Legal Analytic:** applicazioni che abilitano 1) la costruzione di sistemi proattivi che supportano gli utenti nel prendere decisioni e 2) l'analisi avanzata dei dati attraverso la realizzazione di Dashboard personalizzate

Queste applicazioni supportano l'utente (Avvocati e General Consuel) durante il ciclo di vita di gestione di una pratica legale (agevolando la strategia e la lavorazione della pratica stessa) e nella gestione della struttura Legale.

4.2.1. Legal Automation

Durante il ciclo di lavorazione della pratica legale, la possibilità di automatizzare una serie di attività svolte normalmente in maniera manuale, è sicuramente un valore aggiunto in termini di miglioramento della produttività. Nell'ambito delle applicazioni per l'analisi automatica del testo in ambito legale, le tecniche basate su IA e NLP permettono di:

- individuare le parti e le sezioni che lo compongono: i documenti legali possono presentare sezioni definite (es. Intestazione, Parte Consiglio, ecc.), ognuna delle quali ha un contenuto informativo specifico
- riconoscere le entità presenti in esso: all'interno dei documenti legali ci possono essere molti tipi di entità (es. Persona, Luogo, Autorità Giudiziaria, Organizzazione, Persona Legale, Sentenza, Legge)
- identificare Topic/Concetti, ovvero riconoscere gli argomenti di cui parla il documento legale
- estrarre le keyword, ovvero recuperare le parole chiave che caratterizzano il documento
- recuperare gli atti e i documenti simili

I dati e i contenuti (sia strutturati che non) sono raccolti dapprima in formato grezzo in un **Legal Date Lake**, e poi trasformati ed arricchirli in un **Legal Data Hub**. In questo modo si viene a creare un accesso unico, interconnesso e interoperabile alle informazioni.

4.2.2. Legal Discovery

Un asset importante dell'introduzione dell'Intelligenza artificiale nell'ambito legal è rappresentato dall'evoluzione dei motori di ricerca che, partendo da keyword based, si spingano verso un approccio "cognitive" che contestualizzi l'informazione. È necessario, quindi, abilitare una ricerca che selezioni i risultati per comprendere il significato della frase o dei termini che si utilizzano come chiave, producendo risultati veloci e accurati. Si parla di **Legal Discovery**, attraverso la quale è possibile ricercare in maniera intelligente i documenti legali presenti nella Legal Knowledge Base.

L'applicazione di Legal Discovery permettono di:

- favorisce l'integrazione e l'esplorazione di fonti informative non strutturate interne ed esterne all'area legale
- favorisce la diminuzione di tempi e costi nella ricerca, nella gestione del contenzioso
- abilita l'emersione di insight (similarità tra documenti, interconnessione giuridica)

4.2.3. Legal Analytic

Le applicazione di **Legal Analytic** introducono l'AI nell'ambito legale per consentire analisi qualitative al fine di supportare la strategia legale nella gestione dei processi e delle pratiche legali.

Attraverso questa applicazione si mettono a disposizione nuovi **Sistemi di supporto alle decisioni strategiche** costruiti grazie alla realizzazione di modelli e funzionalità di analisi qualitativa avanzata delle informazioni basate su sistemi data-driven e di AI.

Le funzionalità di Legal Analytic si implementano attraverso **Dashboard avanzate** che facilitano il recupero degli *insight* facilitando e automatizzando la visualizzazione di ingenti moli di dati eterogene. L'applicazione di Legal Analytic, in sintesi:

- permette di costruire informazioni quale valido supporto analitico operativo di cui beneficerà l'intera organizzazione
- supporta le decisioni strategiche della struttura legale, come nuovi modelli organizzativi, processi di lavoro alternativi, arricchimento di competenze, strategie legali, ecc.
- definisce un sistema integrato di monitoraggio e controllo per verificare l'andamento dei processi interni, dei costi sostenuti, delle tipologie di controversie gestite e dello stato di lavorazione, al fine di supportare l'individuazione di possibili miglioramenti
- crea un circolo virtuoso anche con gli obiettivi di Performance che ogni anno si dà l'Organizzazione.

4.3. Settore -HR – Anonimizzazione dei dati (Experis)

Per rispettare i vincoli introdotti dal GDPR, preservare la privacy degli utenti e massimizzare la resa dei dati in nostro possesso, risulta molto utile generare nuovi dati anonimizzati. Mentre le classiche tecniche di anonimizzazione basate sulla sanificazione non resistono agli attacchi di re-identificazione, le tecniche di generazione di dati sintetici garantiscono di nascondere il dato originale e escludere gli outlier.

I dati sintetici, oltre a permettere di condividere i dati all'esterno, permettono anche di irrobustire gli algoritmi addestrati sui nuovi dataset. Grazie alla generazione di dati più omogenei e bilanciati è possibile evitare l'overfitting dei modelli sul dataset originale. Allo stesso tempo, inserendo del rumore, è possibile ottenere modelli più efficaci sulla generalizzazione.

Usando algoritmi basati su reti neurali generative (Generative Adversarial Neural Networks, Variational AutoEncoders) è possibile sintetizzare nuovi dati e addestrare gli algoritmi di forecasting per prevedere l'andamento della domanda e dell'offerta del mondo del lavoro. L'utilizzo di dati sintetici permette di moltiplicare le potenzialità dei dati di Experis e fornire solide previsioni sullo sviluppo delle risorse sul mercato.

Una volta generato un nuovo dataset sintetico, i dati al suo interno sono completamente scollegati dal dato originale e permettono all'utente di svincolarsi dalle condizioni di utilizzo e conservazione del dato originale. Questo vantaggio permette di avere un dataset solido perché invariabile nel tempo ma allo stesso tempo malleabile perché può essere generato secondo le necessità di utilizzo.

I dataset sintetici aiutano Experis, come agenzia per il lavoro, ad ottimizzare le procedure di gestione dei candidati, mantenendo alti livelli di rispetto della privacy e riciclando i dati già in suo possesso rendendoli esponenzialmente più efficaci.

4.4. IA per il mondo per i processi HR e il mondo del lavoro (Engineering)

Gli operatori di HR coinvolti nei processi di riconciliazione di domande e offerta di lavoro, sono chiamati oggi a rispondere ad importanti sfide: tra queste, l'evoluzione continua delle professionalità, legata alla necessità di innovare i mestieri, per renderli più efficienti, competitivi e qualitativamente apprezzati a fronte, al contempo, di un progressivo invecchiamento della popolazione. L'innovazione porta con sé la necessità di una riqualificazione progressiva della manodopera per la creazione di nuove professionalità, che raramente si inquadrano nelle definizioni proposte dalle tassonomie nazionali usate a supporto dell'Incontro tra Domanda e Offerta di lavoro, statiche e spesso obsolete. In questo contesto, la sola valutazione di informazioni strutturate (dunque tabellari, basate su codifiche predefinite) fornisce un approccio limitativo, che consente di valutare in modo parziale l'informazione, limitatamente al grado di corrispondenza tra il profilo di un CV e schemi predefiniti. In questo contesto, l'Intelligenza artificiale (AI) si configura come uno strumento a supporto della ricerca di impiego, su diversi fronti.

Supporto all'estrazione e all'immissione di informazione: l'IA consente di personalizzare e semplificare le ricerche a supporto del cittadino, da un lato, e rendere più efficienti i processi di backoffice, dall'altro. Coniugando tecniche di image processing ed information extraction è possibile automatizzare l'estrazione delle informazioni contenute in documenti nativamente digitali o da scansioni, rendendoli ricercabili ed evitando al cittadino l'inserimento di informazioni multiple all'interno su piattaforme differenti. Lo stesso processo evita un ingente lavoro data entry manuale da parte degli operatori a supporto, consentendo loro di focalizzarsi sulla validazione dell'informazione disponibile. L'estrazione automatica di informazioni da documenti, nei loro formati reali e non ottimali, sia in termini di supporto: ad esempio scansione invece che file editabili, che di formato: ad esempio CV in formato non europeo standard, è il primo passo per successive ricerche che mettono in corrispondenza la domanda e l'offerta di lavoro, sia con metodi classici basati su query, che con metodi avanzati che fanno ricorso ad algoritmi di matching sfumato.

Profondità informativa: l'uso di tecniche di NLP consente di estrarre informazioni sia da campi strutturati (in formato tabellare o semi-tabellare), sia da campi non strutturati (descrizioni in linguaggio naturale), integrando ad approcci tradizionali, basati sulla rispondenza di un profilo rispetto a tassonomie consolidate. L'uso di modello "cognitivi", basati sul Deep Learning, consente di comprendere il testo contenuto ed associare a concetti ed entità descrizioni apprese in modo "data-driven", seppur sotto il costante governo dell'Utente.

Potenza nella ricerca: l'integrazione di sistemi di ricerca basati sull'uso del Deep Learning e di Modelli Linguistici, che estendano le tradizionali rappresentazioni tassonomiche, consente di superare le ricerche per parole chiave. La rappresentazione della conoscenza sotto forma di astrazioni matematiche favorisce il superamento delle barriere linguistiche e lessicali, favorendo la riconciliazione tra basi dati differenti. La rappresentazione interna complessa consente la messa a punto di sistemi di ricerca che affianchino alla tradizionale suddivisione in campi ma consentono di valutare i profili in modo "olistico", sulla base di profili generati algoritmicamente a partire dalla base dati a disposizione.

Creazione di percorsi di formazione personalizzati: il potenziamento dei sistemi di ricerca, e la creazione di profili professionali che siano definiti anche dall'informazione presente, consente di proporre tramite l'applicazione di algoritmi previsionali (forecasting) dei percorsi di crescita personalizzati, sulla base del confronto di profili e competenze simili, favorendo attività di reskilling.

Previsione dei volumi di domanda e offerta di lavoro, del turnover e della disponibilità di risorse: i sistemi predittivi possono essere impiegati per prevedere la richiesta e la potenziale offerta di manodopera, basata su variabili endogene all'Ente o esogene (fattori macroeconomici, costi dell'energia, fiducia dei consumatori, successo di un prodotto ecc.). Qualora un simile sistema analitico venisse impiegato per pianificare l'allocazione di risorse umane ed economico, consentirebbe una ottimale pianificazione dei turni di lavoro e dell'allocazione del personale, in modo da rendere l'organizzazione del lavoro più efficace, aumentando il valore della produzione.

Analisi avanzate sul fenomeno: grazie all'analisi di CV e di Job Vacancies e alla valutazione di campi numerici e strutturati, a partire dall'informazione a disposizione è possibile monitorare costantemente il volume di richieste, posizioni aperte, skill, valutarne l'andamento e, tramite algoritmi di forecasting, definire degli scenari previsionali, che possano essere forniti ai policy makers per orientare in modo efficace politiche future per il lavoro.

Nel campo dell'HR, l'uso di tecniche di IA non va inteso come mera applicazione di opachi algoritmi in ottica prescrittiva a sostituzione del ruolo degli operatori. Al contrario, un sistema di Intelligenza artificiale andrebbe inteso come un acceleratore di processi, che, by design dovrebbe risultare almeno:

- spiegabile (explainable), ovvero in grado di produrre anche una spiegazione del proprio output, interpretando e quantificando la ragione delle proprie decisioni alla luce dei risultati prodotti, senza però banalizzare il complesso processo di inferenza, tipico dei sistemi artificiali adattivi;
- responsabile (accountable), implementando tutte le misure necessarie ad avere un software robusto, in grado di ricondurre in modo netto l'utente all'origine di ogni decisione;
- equo (fair), in grado di essere resiliente ad eventuali bias, garantendo piena accessibilità agli utenti, segnalando agli operatori potenziali distorsioni nei risultati.

A partire da questi presupposti, l'uso di Intelligenza artificiale consente di superare i limiti offerti dagli strumenti software tradizionali, innovando i processi e fornendo potenti strumento di Governance, orientato a fornire delle misure quantitative sul mercato del lavoro e a facilitare l'adozione di misure a supporto di lavoratori e imprese.

4.5. IA per il risparmio energetico (Engineering)

L'energia è uno dei fattori chiave per lo sviluppo economico e il benessere delle persone, ma la sua crescente domanda ha anche un impatto significativo sull'ambiente e sul cambiamento climatico. Di conseguenza, il risparmio energetico è diventato un obiettivo importante per molte organizzazioni e governi di tutto il mondo e in questo contesto l'Intelligenza artificiale (IA) sta emergendo come una tecnologia cruciale per supportarlo. L'IA può infatti essere utilizzata per monitorare e ottimizzare l'uso dell'energia in tempo reale, ridurre gli sprechi e le perdite, ridurre le emissioni di gas serra e prevedere i consumi futuri. È dunque in crescita il numero di applicazioni reali dell'IA in questo ambito, tra cui: la gestione dell'energia domestica, l'automazione industriale, la gestione intelligente degli edifici, la manutenzione predittiva o la pianificazione energetica a livello nazionale a breve e lungo termine.

- **Previsione della domanda e dell'offerta di energia elettrica e gas**:

l'IA può essere utilizzata per analizzare enormi quantità di dati di domanda e offerta di energia, in modo efficiente e veloce, e per identificare i pattern nascosti e le relazioni tra le variabili che la influenzano. Queste informazioni possono essere anche utilizzate per generare previsioni accurate sulla domanda e l'offerta di energia a breve e lungo termine. Le previsioni consentono una migliore gestione e ottimizzazione delle risorse energetiche, una maggiore affidabilità della fornitura di energia e una riduzione delle emissioni di gas serra. In particolare, un ampio uso di queste tecniche è utilizzato per la stima della generazione dell'energia prodotta da impianti solari ed eolici, in cui le variabili meteo, le caratteristiche del singolo impianto e le grandezze meteo sono le componenti principali per definire una stima accurata.

- **Ottimizzazione e controllo delle reti elettriche (e gas)**:

l'ottimizzazione e il controllo delle reti elettriche e del gas possono aiutare a migliorare l'efficienza energetica, ridurre i costi, migliorare la qualità della fornitura di energia, contribuire a una maggiore adozione e integrazione delle fonti di energia rinnovabile. Ad esempio, per le reti elettriche la quantità di potenza immessa deve essere uguale alla quantità di potenza consumata in ogni momento e i flussi di potenza risultanti devono soddisfare i vincoli dettati dalla topologia della rete. L'ottimizzazione delle reti elettriche diventa ancora più complessa in contesti che prevedono una grande quantità di impianti da fonti rinnovabili la cui produzione è certamente più aleatoria, variando in base alle condizioni meteorologiche e ambientali. In tale contesto l'IA propone diversi approcci innovativi per monitorare in tempo reale le reti, raccogliere dati sui consumi di energia, le condizioni ambientali, le attività industriali e altri fattori che ne influenzano il funzionamento.

Questi dati possono essere utilizzati per intervenire su diversi aspetti: prevedere i picchi di domanda, ridurre le perdite di energia e gestire la distribuzione dell'energia in modo più efficiente. In particolare, l'IA può essere utilizzata per creare modelli di simulazione delle reti elettriche (analogamente, può valere per quelle del gas), che consentono di testare diverse strategie di gestione e di prevedere gli effetti delle decisioni. Questi modelli possono aiutare a individuare le aree della rete in cui si verificano problemi di sovraccarico o perdite o sprechi di energia e a sviluppare soluzioni mirate per risolvere questi problemi. Inoltre, l'IA può essere utilizzata per creare algoritmi di controllo automatico della rete, che consentono di monitorare e regolare la produzione

e la distribuzione di energia in tempo reale. Questi algoritmi possono essere utilizzati per gestire le reti in modo più efficiente, prevenire i blackout, ridurre gli sprechi e garantire la stabilità della rete elettrica.

- **Massimizzazione della generazione di energia rinnovabile**:

il problema dell'inseguimento del punto di massima potenza (MPPT) mira a ottimizzare le configurazioni degli impianti di energia da fonti rinnovabili al fine di aumentarne la produttività. In tale contesto l'IA propone diversi approcci innovativi come ad esempio: orientare i pannelli solari mobili tramite l'uso di reti neurali addestrate a massimizzare il loro utilizzo in funzione della radiazione solare diretta, riflessa e diffusa; riconfigurare le topologie dei pannelli solari per tenere conto dell'ombreggiatura, utilizzando un approccio di rete neurale supervisionata per mappare i valori di irradianza a topologie potenziali; utilizzare delle reti neurali per controllare la velocità di rotazione dell'albero di una turbina eolica per massimizzare la potenza senza richiedere misurazioni della velocità del vento.

- **Monitoraggio dei consumi elettrici domestici**:

in ottica dei consumi elettrici domestici, l'IA permette diversi approcci innovativi, uno dei più importanti riguarda la realizzazione di soluzioni di tipo NILM (Non Intrusive Load Monitoring), che offre sia ai proprietari degli appartamenti che ai gestori di edifici la possibilità di identificare i singoli device/elettrodomestici presenti nell'abitazione e di monitorarne il consumo, con una minima invasività nella casa: un solo modulo a valle del contatore, trasmette dati ad algoritmi remoti. In questo modo, non è necessario installare sensori dedicati distribuiti su un'intera casa o edificio per uffici. Di fatto, partendo dal dato aggregato, una soluzione NILM, mediante l'utilizzo di algoritmi di ML, separa le firme energetiche di ciascun dispositivo dal consumo energetico complessivo. Quindi, sulla base del segnale elettrico aggregato ricevuto in input consente di: identificare gli elettrodomestici attivi in un certo periodo, individuandone accensione e spegnimento dei singoli device; valutare i consumi, in termini sia elettrici che economici, per ogni dispositivo in funzione; valutare il funzionamento del device, permettendo di rilevare anomalie ed eventuali guasti. Inoltre, l'IA potrebbe analizzare i dati di utilizzo degli elettrodomestici per prevedere i momenti di picco dell'energia elettrica così da regolare

automaticamente l'uso dei diversi dispositivi al fine di evitare picchi di energia e migliorare l'efficienza energetica della casa. Queste informazioni possono essere estremamente utili sia lato consumatore che lato fornitore, in quanto possono offrire anche spunti di risparmio energetico o di ottimizzazione dei consumi.

- **Progettazione di sistemi di controllo energetico nell'edilizia e Smart Building**:

anche nell'ambito dell'edilizia possono essere applicate nuove soluzioni che aiutino a gestire meglio i consumi energetici e a ridurre gli spechi. Infatti, come per il consumo domestico, attraverso la raccolta dei dati storici si possono realizzare modelli di ML per la previsione del consumo energetico degli edifici. In questo caso l'AI può basarsi su fattori come il tempo, la stagione, il tipo di edificio e le informazioni strutturali per la previsione futura dei consumi che di fatto può essere di grande aiuto per poter adottare misure preventive per la riduzione e quindi il risparmio energetico. Inoltre, questo approccio aiuta anche a identificare schemi di consumo anomali, non tipici dell'edificio per tipologia e/o struttura, e che possono essere indicativi di problemi o inefficienze, aiutando a individuare e risolvere i problemi di consumo in modo tempestivo. Negli edifici si può prevedere anche l'uso di contatori intelligenti per migliorare l'efficienza energetica che tramite tecniche di ML che analizzano i dati raccolti possono identificare modelli di consumo dell'utente e proporre soluzioni alternative per ridurlo (riducendo così anche i costi associati). Questo ovviamente non solo relativamente al consumo dei dispositivi elettrici in casa, ma anche con sistemi di controllo che, ad esempio, permettono di monitorare i consumi del gas per il riscaldamento. Abbinando queste informazioni con l'uso di altre tecnologie, come video/droni e termocamere, è possibile mettere in relazione i dati di consumo dei riscaldamenti con il monitoraggio delle dispersioni di calore degli edifici, consentendo ai modelli di ML di suggerire interventi in zone dell'edificio che permettano di ovviare alla dispersione del calore e migliorare l'efficienza energetica. Anche la gestione della ventilazione e/o climatizzazione degli edifici può essere ottimizzata con l'uso di algoritmi di ML, ad esempio, in base alle condizioni ambientali (es. temperatura e umidità), al movimento dei clienti/utenti, ecc., è possibile prevedere le esigenze di ventilazione e regolando l'apertura delle finestre e delle porte e ottimizzare

il consumo energetico dei sistemi di condizionamento dell'aria programmando gli impianti in modo da tenerli accesi solo quando necessario.

- **Riduzione dei consumi in ambito industriale**:

anche i consumi delle industrie possono essere considerevolmente ridotti se si sfruttano le potenzialità dell'AI. Ad esempio, questa può essere utilizzata per analizzare i dati relativi ai macchinari industriali, come la temperatura, la velocità e la pressione, per ottimizzarne il consumo e ridurre gli sprechi. Le tecniche di ML possono essere utili su molti aspetti: identificare le opportunità di efficienza energetica riducendo le perdite di calore o ottimizzando il carico di lavoro; possono utilizzare i dati raccolti come storico per prevedere il consumo di energia, di fatto consentendo di pianificare in anticipo il consumo futuro e adottando misure per ridurlo in periodi di picco; possono ulteriormente analizzare i dati per individuare schemi anomali e segnalare problemi, guasti e/o malfunzionamenti così da adottare misure preventive. Gli algoritmi di ML possono, ad es., aiutare nell'analisi dei dati relativi al consumo e le prestazioni dei motori elettrici di macchine industriali. Identificare componenti energivori permette di intervenire sugli impianti industriali in modo mirato introducendo dispositivi più efficienti per ridurre il consumo di energia e migliorare l'efficienza produttiva.

Smart city: l'aspetto legato alla riduzione dei consumi energetici cittadini assume un interesse crescente. Tra le molte proposte, le soluzioni di illuminazione pubblica intelligente possono essere basate su tecniche di ML e possono essere realizzate utilizzando sensori per monitorare il consumo energetico delle luci pubbliche in tempo reale e regolare automaticamente l'intensità delle luci in base alle condizioni ambientali (luce del sole) e la presenza di persone e/o il traffico. In questo caso l'IA può essere utilizzata per ottimizzare il consumo cittadino riducendo di molto i costi energetici soprattutto per le zone remote e meno frequentate, ma di fatto senza creare disservizi. Questa tecnologia può essere applicata nei diversi ambiti, infatti può non essere limitata al tema dell'illuminazione pubblica, ma anche ai diversi servizi offerti. Ad esempio, è possibile gestire in modo efficiente l'illuminazione degli impianti sportivi regolando automaticamente l'intensità delle luci in base alle condizioni di luce ambientale o alle attività in corso. Analogamente, anche gli impianti in edifici di pubblica utilità così come privati possono beneficiarne (ad esempio biblioteche, pompe di benzina, ecc.). Algoritmi di IA che lavorano in tempo reale possono essere applicati ai dispositivi elettronici presenti in questi servizi

per ottimizzarne i consumi (ad esempio la luminosità dei televisori in funzione della luce ambientale). L'IA può essere utilizzata anche per monitorare i consumi degli edifici, ad esempio dei centri commerciali, degli hotel, dei ristoranti, ecc. Tutto questo aiuta a identificare le aree in cui si sta consumando troppa energia e diverse soluzioni di riduzione possono includere l'ottimizzazione della temperatura, l'illuminazione e/o l'utilizzo di nuovi elettrodomestici.

4.6. IA per il settore della Sanità (Reply)

La applicazione dell'intelligenza artificiale nel settore Sanità è un elemento che può fornire valore sia alle imprese del settore sia ai pazienti.

La possibilità di applicare l'Intelligenza artificiale si è concretizzata negli ultimi anni, sia a seguito di oggettivi progressi conseguiti nel settore sia nella crescente disponibilità di dati.

Occorre notare come questa disponibilità di dati sia potenzialmente enorme ma in pratica sia limitata da aspetti tecnici (mancanza di interoperabilità, stream di dati acquisiti in modo non omogeneo, assenza di certificazione dei dati, …) e da aspetti regolatori.

Certamente la legislazione europea (GDPR) è più restrittiva di altre e l'AI Act è ancora in fase di messa a punto. In altre aree, come negli US, regolamenti diversi (o assenza di questi) hanno favorito l'adozione della IA nel settore sanitario. Tra le più significative a livello di sistema si può ricordare UnanimousAI[22], azienda americana che ha sviluppato un sistema di Intelligenza artificiale che affianca i medici generici e specialistici nella analisi dei dati clinici e nella diagnostica. Il sistema raccoglie informazioni/esperienze dai medici ogni volta che questi interagiscono con il sistema e raccoglie informazioni dalle centinaia di migliaia di articoli pubblicati ogni anno in tutto il mondo nel settore sanità. Inoltre, accede a banche mondiali su epidemie, infezioni e a banche farmaceutiche mettendo tutti questi dati a disposizione del sistema IA per la loro analisi. Le consultazioni dei medici sono pure esse mediate da sistemi di IA conversazionali.

[22] https://unanimous.ai

Nel seguito si fa riferimento al contesto europeo e più in particolare a quello italiano anche se alcuni dei casi studi riportati hanno trovato applicazione anche in altri stati europei.

Rispetto ai due fattori, tecnico e regolatorio, l'IA deve fornire supporto sul versante tecnico nel rispetto dei vincoli regolatori oggi esistenti.

Un elemento che nella esperienza di Reply Laife è fondamentale è aiutare i clienti a sviluppare una sensibilità sulla applicazione della Intelligenza artificiale, da un lato comprendendone i possibili vantaggi e dall'altra limiti e elementi di cautela.

L'IA non è una panacea, è semplicemente uno strumento di grandi potenzialità il cui corretto sfruttamento è responsabilità di chi lo usa. Per contro, l'utilizzatore deve essere consapevole dei limiti ed essere in grado di analizzare i risultati di cui si assume la responsabilità.

Questo è ancor più necessario in un settore quale la sanità di cui sono evidenti le criticità e gli impatti. Peraltro, e questo è il messaggio forte che si vuole condividere, i benefici portati dalla IA giustificano gli sforzi richiesti per adottare le cautele necessarie.

Il gruppo di lavoro "Digital Transformation in Sanità" di Anitec Assinform ha pubblicato un White Paper che analizza, tra altri aspetti, anche quello della applicazione di IA al settore sanità. Si rimanda a quel White Paper per approfondimenti case study sviluppati da Laife Reply di cui viene qui presentato l'elenco:

- Modelli predittivi per rischio riacutizzazioni
- Corporate Wellbeing
- Digital Twin per l'automazione della "vaccine discovery"
- Digital Twin per la medicina dello sport
- Clinical data platform
- Analisi di immagini cliniche

5. Conclusioni

L'intelligenza artificiale, come mostrano i tanti esempi contenuti in questo White Paper, trova applicazione in moltissimi settori e in tutte le fasi del business: dal percorso "ideazione - studio di mercato – progettazione", alle fasi di produzione, gestione delle risorse (materiali e umane), fino al controllo qualità, *costumer relations* e gestione delle *supply* e *distribution chain*.

Nonostante le grandi potenzialità di applicazione e creazione di valore, la percentuale di aziende che adopera l'intelligenza artificiale in Italia è ancora bassa. Secondo dati ISTAT del 2021, solo il 6,2% delle imprese italiane ha dichiarato di utilizzare sistemi di Intelligenza artificiale, contro una media dell'8% nell'Unione europea. Il dato è spiegato anche – e soprattutto – guardando alle PMI: la percentuale di adozione di IA per queste aziende si attesta al 5,3%, contro il 24,3% delle grandi imprese. Allo stesso tempo, va sottolineato che segnali positivi arrivano dall'ecosistema start-up. In Italia le start-up e le PMI innovative del settore ICT che sviluppano soluzioni di Intelligenza artificiale e machine learning sono stabilmente sopra quota mille e rappresentano oltre il 10% del totale (11,3% dall'ultimo rapporto Anitec-Assinform Infocamere, pagg. 7-8).

In realtà, però, **l'IA è diffusa in molti apparati e sistemi ma ancora non emerge a livello di "consapevolezza".**

La conseguenza di ciò è che l'IA: **non viene usata come leva competitiva** al fine di migliorare efficienza, qualità e rapporto con i clienti.

Spesso la distonia tra "potenzialità" – concrete, come dimostrato dai molti casi d'uso – e "sfruttamento" della tecnologia è dovuta, da un lato, alla richiamata "mancanza di consapevolezza" sia su ciò che l'IA possa fare per l'azienda, dall'altro alla percezione che l'IA sia "troppo complicata" e in qualche modo fuori dalla portata. A ciò contribuiscono vari fattori: l'enfasi data dai media ai rischi dell'IA, a un contesto regolatorio – che, pur essendo in divenire – sembra poco concentrato a guardare alle opportunità di innovazione e al favorirle, a una cultura manageriale diffusa che fatica a concepire l'innovazione digitale come un fattore di competitività.

Occorre, tuttavia, notare che, come evidenziato dalle molte testimonianze raccolte da Anitec Assinform e Confindustria Piccola Industria durante il roadshow "*IA e PMI: Esperienze da un futuro presente*", esistono molte piccole medie aziende che, non solo utilizzano l'IA, ma sono parte attiva nella sua

evoluzione nei più svariati settori applicativi e che rappresentano, in termini di applicazione, delle eccellenze a livello internazionale.

Una "radice" importante alla base del divario tra potenzialità e effettivo sfruttamento in ambito IA si trova nella mancanza di **risorse umane preparate in modo pragmatico all'applicazione dell'IA**.

Gli *output* di ricerca delle Università italiane dimostrano che nel nostro Paese il livello della ricerca accademica non è distante da quello degli altri principali Stati europei. Tuttavia, nonostante vi siano sempre più importanti progettualità per favorire il trasferimento tecnologico dall'Università al mercato, rileviamo un orientamento ancora troppo teorico e scarsamente improntato alla soluzione di problemi di *business*.

L'applicazione dell'IA in questa fase storica – e ciò varrà ancora di più nel futuro – passa anche attraverso la preparazione di professionisti dotati di un *background* formativo di tipo tecnico. Quest'ultimo è un elemento che ci vede da sempre in prima linea, con proposte operative per potenziare il sistema degli ITS. Auspichiamo di poter cogliere già nel medio periodo i frutti degli sforzi importanti che il legislatore ha fatto negli ultimi anni per potenziare questo tipo di percorsi. L'industria ha bisogno di risorse preparate ad utilizzare gli strumenti messi a disposizione dalla IA.

Non ci confrontiamo, tuttavia, solo un problema di mancanza di competenze aziendali ma anche con un problema di approccio all'evoluzione dell'azienda.

La transizione digitale, il metaverso e i *data spaces*, sono tre elementi di cui si parla molto ma che non trovano ancora un'adeguata "metabolizzazione" nella cultura aziendale e di management strategico. Anche su questo versante una formazione strategica, sia nel pubblico che nel privato sarà sempre più importante. La transizione digitale "sposterà" le attività nel "metaverso" – *consumer*, ma soprattutto industriale, e questo comporta un ripensamento dei processi, e una parallela rivisitazione della gestione delle risorse umane.

La pandemia ha dimostrato come sia stato possibile, con tecnologie da tempo disponibili, organizzare gran parte dell'attività lavorativa nel *cyberspace*. Se per moltissime aziende in molti settori questo processo ha rappresentato un punto di svolta nel modo di fare business e di gestire e usare le risorse; per alcune è stata solo una parentesi.

La comunicazione e la costruzione di valore sui dati hanno rappresentato per molte aziende un vero e proprio cambio di prospettiva. Non solo dati necessari

a gestire il business ma dati come fonte di business. L'Intelligenza artificiale è uno strumento cruciale sia per la gestione sia per trasformare i dati in valore.

Anitec Assinform continuerà il suo ruolo di catalizzatore nella diffusione della IA specie verso le PMI che sono quelle che più possono guadagnare dalla IA e certamente quelle più a rischio di essere tagliate fuori da chi l'IA la usa.

Questo vale anche a livello delle singole persone: Nonostante ci sarà uno spiazzamento in alcune professioni con l'avvento dell'Intelligenza Artificiale, il pericolo maggiore che intravediamo sia per le aziende che per i lavoratori è legato alla perdita di competitività. Chi adotta per primo, e in modo efficace, le tecnologie basate sull'IA guadagnerà un vantaggio significativo sul mercato. Questa dinamica avrà impatti sull'occupazione che è essenziale considerare.

In conclusione, va espressa una riflessione sul tema della Regolazione europea dell'IA nel contesto della competizione globale su questa tecnologia. In Europa, l'AI Act inizierà ad applicarsi tra il 2026 e il 2027. Vista la crescita del mercato e dell'ecosistema dell'IA, il regolamento si applicherà su un numero di imprese e utenti ben maggiore rispetto al panorama di oggi. L'impatto dell'AI Act sarà determinante su tantissime realtà aziendali dell'*offerta* (da multinazionali a start-up) ma in generale su tutto il sistema produttivo, che sempre di più utilizza Intelligenza artificiale per migliorare prestazioni ed efficienza.

Nei prossimi anni, quindi, le imprese dovranno impegnarsi per assicurare la *compliance* dei loro prodotti al Regolamento. Per adeguarsi al AI Act senza sacrificare le prestazioni dei sistemi e la capacità di investimento, sarà fondamentale che i negoziati non perdano di vista la fattibilità commerciale e la fattibilità tecnica norme che saranno stabilite.

La Commissione europea sta puntando sempre di più sul cd. *Effetto Brussels*: vale a dire la capacità di influenzare lo sviluppo di prodotti a livello globale imponendo norma che si applicano sul vasto mercato europeo. Tuttavia, è da dimostrare che per l'IA tale dinamica si riproduca. Infatti, le altre grandi potenze coinvolte nella *AI Race* globale, che sono molto più avanti dell'Europa per investimenti e ricerca, stanno propendendo per approcci più *soft* (USA) o comunque con un ambito di applicazione più ristretto (Cina).

Se è difficile immaginare di poter tenere il passo dei *leader* mondiali solo imponendo regole, allora è fondamentale che il Regolamento si iscriva in un disegno strategico ampio: fatto di investimenti in infrastrutture digitali, ricerca, tecnologia e formazione, sia specialistica che di base. Solo così, l'Europa potrà

aspirare a competere con le grandi potenze dell'IA, sfruttando al meglio le potenzialità di questa tecnologia per il proprio sviluppo socioeconomico.