Intelligenza artificiale: dalla geopolitica alla fabbrica.

Regole, infrastrutture e industria per il sistema produttivo italiano



Realizzato dall'Ufficio Studi AIdAM

Versione 1 – Ottobre 2026

Associazione Italiana di Automazione Meccatronica
Viale Fulvio Testi, 128 - 20092 Cinisello Balsamo (MI) - Tel. +39 02 24416431
Cod.fisc.97247340157 - P.IVA 08552740964 www.aidam.it - segreteria@aidam.it

Indice della pubblicazione:

Prefazione alla pubblicazione 5

Capitolo 1 – Alle basi dell'AI: il machine learning 6

1. Il cambio di paradigma nell'informatica moderna 6
2. Dalle tavolette babilonesi alla macchina di Turing: una genealogia del calcolo 7
3. Il machine learning: quando la macchina impara dagli esempi 9
4. Reti neurali e deep learning: architetture dell'intelligenza artificiale 11
5. I large language model (LLM) e la generazione di testo 14
6. I tre pilastri del successo del deep learning 15
7. Applicazioni emblematiche: da AlphaFold a Vista 16
8. Il lavoro nell'era dell'intelligenza artificiale 17
9. Machine learning e programmazione tradizionale: una complementarità necessaria 18
10. Riflessioni conclusive: potere, responsabilità e futuro 19

Capitolo 2 – La penetrazione dell'AI nel sistema industriale italiano 21

1. L'intelligenza artificiale: una tecnologia di sistema 21
2. La fotografia dell'adozione in Italia 22
3. Come le imprese italiane usano l'IA: 241 casi concreti 24
4. Nel cuore delle aziende: un atlante delle funzioni aziendali 28
5. La penetrazione settoriale: dove l'AI sta già cambiando la produzione 33
6. Cinque lezioni dall'esperienza delle imprese 39
7. Il quadro normativo europeo: l'AI Act e i suoi effetti 40
8. Prospettive e priorità per l'Italia 43

Capitolo 3 – La mappa mondiale dell'AI: la dimensione geopolitica dell'intelligenza artificiale 45

1. L'intelligenza artificiale come posta in gioco geopolitica 45

2. Il capitalismo politico: quando la sicurezza nazionale governa l'economia 46
3. L'ecosistema dei semiconduttori: filiere, nicchie e guerra invisibile 48
4. La materialità dell'intelligenza artificiale: data center, energia e filiere 51
5. Dipendenze strutturali e potere di mercato 54
6. Punti di forza e vulnerabilità delle due potenze 55
7. Le terre rare: il sottosuolo che governa l'intelligenza artificiale 56
8. Prospettive: la mappa del futuro prossimo 61
Capitolo 4 – Regolare l'Intelligenza Artificiale 63
1. Tre potenze, tre filosofie normative 63
2. L'architettura dell'AI Act: un regolamento basato sul rischio 65
3. Le criticità del modello europeo 68
4. Oltre la forma: le questioni sostanziali ancora aperte 70
5. Considerazioni di sintesi 72
Capitolo 5 – La cybersecurity ai tempi dell'AI 73
1. Un'escalation senza precedenti: il panorama della minaccia cyber 73
2. L'anatomia del cybercrime contemporaneo 75
3. Verso una valutazione dinamica del rischio cyber 77
4. L'IA a supporto della gestione degli incidenti: il caso PACY 78
5. Riflessioni conclusive e prospettive 81
Capitolo 6 – L'Italia dei data center 83
1. I data center: l'infrastruttura fisica dell'intelligenza artificiale 83
2. La sfida energetica: quadruplicare i consumi senza destabilizzare il sistema 84
3. I data center come opportunità: valore economico, occupazione e circolarità 87
4. Governance, pianificazione e ruolo istituzionale 90

5. Considerazioni conclusive 92
Manifesto dell'AI e della Robotica 94
Fonti utilizzate 96
ALLEGATI – Case study delle aziende AIdAM 98
Case History 1 – Awentia Srl 98
Case History 2 – HumanQ Srl 109

Prefazione alla pubblicazione

Il tema dell'intelligenza artificiale è attuale, divisivo, inflazionato. Trattandosi di una delle più notevoli rivoluzioni tecnologiche che l'essere umano abbiamo mai affrontato, è auspicabile che sia sulla bocca di tutti. Attraendo anche innumerevoli capitali, come vedremo nel documento, rende appetibile la fertilizzazione di un tessuto di professionisti, in forma individuale o organizzati in piccole aziende, che si collocano come esperti della materia, pur esprimendo i medesimi concetti che leggiamo sulle riviste e che ascoltiamo nei numerosi convegni che affollano le sale di tutto il mondo.

L'Ufficio Studi AIdAM ha voluto dare corpo ad un documento che fonda sui contenuti e sulle fonti la vera consistenza di ciò che rappresenta oggi l'AI. AIdAM ha lavorato per mesi all'individuazione delle voci più autorevoli e delle indagini più accreditate, all'analisi dei documenti di maggior valore su questo innovativo tema e alla finalizzazione, all'interno di una pubblicazione unica, dello stato dell'arte dell'intelligenza artificiale, a quattro anni dalla sua trasformazione in strumento di massa (il lancio di Chat GPT 3.4). Ci si è concentrati su livello di penetrazione dell'AI nel tessuto industriale italiano, offrendo uno spaccato sia per singoli settori merceologici, sia all'interno delle diverse funzioni aziendali; si è dedicato uno spazio agli impatti economici dell'AI nei diversi continenti, con tutti gli effetti di geopolitica che ne conseguono. Sono state approfondite le minacce e le opportunità che questo "new high tech deal" porta con sé, non a livello macroeconomico, bensì per l'industria italiana e quindi per il nostro tessuto imprenditoriale. Non ultimo è stato dedicato spazio al tema dei data center che, se da un lato permette di rendere fisico (infrastrutture, capannoni) quello che è percepito come intangibile (algoritmi, software), dall'altro alimenta una spirale di investimenti e mette in moto una filiera che può essere di notevole sviluppo per il mondo dell'automazione.

Infine, ma non ultimo, forti del nuovo gruppo costituito all'interno dell'Associazione dedicato all'ambito "Software, AI, Umanoidi", abbiamo voluto portare dei case study di come e cosa le aziende AIdAM hanno già sviluppato e rendono disponibile sul mercato su questo tema. Perché mentre il mondo presenta questa tecnologia come il futuro, l'automazione la vive nel presente.

Capitolo 1 – Alle basi dell'AI: il machine learning

1. Il cambio di paradigma nell'informatica moderna

Per gran parte della storia del calcolo automatico, la relazione tra l'essere umano e la macchina è stata unidirezionale e gerarchica: l'uomo fornisce istruzioni precise, la macchina le esegue fedelmente. Questo modello, noto come programmazione imperativa, ha dominato l'informatica per decenni, producendo sistemi straordinariamente potenti ma intrinsecamente rigidi. La potenza di tali sistemi risiedeva nella capacità di eseguire operazioni complesse con velocità e precisione inumane, ma la loro intelligenza rimaneva quella prestata dal programmatore, non qualcosa che la macchina fosse in grado di sviluppare autonomamente.

Il confronto tra due storiche sfide nel mondo degli scacchi e del gioco del Go illumina con straordinaria chiarezza questo cambiamento epocale. Nel 1997, quando Deep Blue sconfisse Garry Kasparov — campione mondiale in carica — nel gioco degli scacchi, il risultato fu il frutto di anni di lavoro ingegneristico: un sistema capace di valutare milioni di posizioni al secondo grazie a regole esplicitamente codificate da programmatori ed esperti del gioco. Deep Blue non imparò nulla dalla partita; applicò semplicemente, a velocità prodigiosa, le istruzioni ricevute.

Il Go rappresentava invece una sfida di natura diversa, quasi filosofica. Le sue regole sono più semplici rispetto agli scacchi, ma il numero di configurazioni possibili supera il numero di atomi nell'universo osservabile. Questo rendeva inapplicabile l'approccio "brute-force" che aveva consentito a Deep Blue di eccellere. Per vent'anni, i maestri di Go mantennero la supremazia sull'intelligenza artificiale grazie a quella facoltà, l'intuizione — la capacità di percepire in un colpo d'occhio la qualità posizionale di una configurazione — che nessun algoritmo tradizionale riusciva a replicare.

Nel 2017, tutto cambiò. AlphaGo, sviluppato da DeepMind (Google), sconfisse Ke Jie, il campione mondiale in carica. Ma la vera rivoluzione non era nella vittoria in sé, bensì nel metodo: AlphaGo non era stato programmato per giocare a Go. Era stato addestrato su milioni di partite, assimilando pattern, strategie e sfumature che nessun programmatore avrebbe saputo formalizzare esplicitamente. La macchina aveva imparato, nel senso più autentico del termine.

Ancora più sorprendente fu la velocità del progresso. Mentre la creazione di Deep Blue aveva richiesto circa dodici anni di sviluppo intensivo, AlphaZero — una versione generalizzata capace di padroneggiare scacchi, Go e Shōgi — raggiunse il livello del miglior programma scacchistico al mondo in appena quattro ore di autoapprendimento. Questo balzo temporale non è semplicemente un indicatore di maggiore efficienza: segnala un cambio qualitativo nel tipo di intelligenza artificiale che siamo in grado di costruire.

2. Dalle tavolette babilonesi alla macchina di Turing: una genealogia del calcolo

2.1 Gli algoritmi come eredità culturale

Il termine "algoritmo" porta con sé una storia millenaria che attraversa civiltà e continenti. Le prime procedure sistematiche per la risoluzione di problemi matematici compaiono su tavolette babilonesi databili tra il 1800 e il 1600 a. C., e su papiri egizi di poco successivi. Ma la parola stessa deriva dalla latinizzazione del nome di Al-Khwarizmi, matematico e studioso arabo che, intorno all'825 d.C., diresse la leggendaria Casa della Saggezza di Baghdad e scrisse il primo trattato sistematico sul sistema numerale indiano.

Fu grazie a Leonardo Fibonacci che questi strumenti intellettuali raggiunsero l'Europa. Vissuto a lungo nel Nord Africa per ragioni commerciali, Fibonacci entrò in contatto con la tradizione matematica araba e, nel 1202, pubblicò il *Liber Abaci*, un'opera monumentale che rendeva accessibili a tutti — non solo ai matematici — i metodi di calcolo basati sulla notazione posizionale. I banchieri furono tra i primi ad adottarla, trovando nei nuovi numeri uno strumento insostituibile per calcolare gli interessi; ma la novità fu osteggiata dalle autorità: a Firenze, nel 1299, uno statuto comunale arrivò a proibire l'uso delle cifre indiane nei libri contabili, episodio che ricorda — con ironia storica — certi odierni tentativi di regolare le tecnologie digitali.

Un algoritmo, nella sua essenza, è una procedura finita che attraverso passi elementari e ben definiti consente di risolvere una classe di problemi. Questa caratteristica di universalità — il fatto che il risultato sia indipendente da chi esegue la procedura — ha reso naturale, fin dall'antichità, il tentativo di delegarne l'esecuzione a meccanismi artificiali.

2.2 Macchine che calcolano: da Anticitera a Babbage

Il primo calcolatore analogico di cui abbiamo conoscenza fu recuperato nel 1900 al largo dell'isola greca di Cerigotto: la macchina di Anticitera, un sofisticato meccanismo a ingranaggi risalente al I-II secolo a. C., capace di prevedere la posizione dei pianeti, le fasi lunari, le eclissi e persino il calendario delle Olimpiadi. Decifrata pienamente solo negli anni Settanta del Novecento grazie a tecnologie di imaging avanzate, questa macchina testimonia quanto profonda fosse l'aspirazione umana ad automatizzare il pensiero matematico.

Nel XVII secolo, Blaise Pascal costruì la prima calcolatrice meccanica capace di eseguire addizioni e sottrazioni. Ma fu Charles Babbage, nella prima metà dell'Ottocento, a concepire qualcosa di qualitativamente diverso: la macchina analitica, un dispositivo programmabile in grado di eseguire operazioni diverse a seconda delle istruzioni fornite. Pur non essendo mai stata costruita per intero, la macchina analitica fu il vero precursore concettuale del computer moderno.

Ada Byron, figlia del poeta Lord Byron, collaborò con Babbage traducendo e ampliando un articolo del matematico Luigi Federico Menabrea sulle applicazioni della macchina analitica. Le sue annotazioni, che superarono in lunghezza il testo originale, contengono quello che viene generalmente considerato il primo algoritmo della storia pensato per essere eseguito da una macchina. Ada comprese inoltre che la macchina analitica avrebbe potuto operare non solo su numeri ma su qualsiasi oggetto rappresentabile simbolicamente — intuizione straordinariamente moderna, che anticipa di un secolo il concetto di computer universale.

2.3 Alan Turing e il fondamento teorico del calcolo

Il passo decisivo verso il computer moderno fu compiuto nel 1936 da Alan Turing, che affrontò il problema della decidibilità proposto dal matematico David Hilbert — l'esistenza di una procedura automatica per dimostrare qualsiasi teorema matematico — costruendo un modello teorico di macchina capace di simulare qualsiasi algoritmo. La macchina di Turing non fu mai realizzata fisicamente, ma fornì il fondamento teorico su cui si basa tutta l'informatica moderna: qualsiasi problema che possa essere risolto algoritmicamente, può essere risolto da questa macchina astratta.

Turing contribuì anche a gettare le basi filosofiche dell'intelligenza artificiale. Nel 1950 propose il celebre test che porta il suo nome: se un giudice umano, interagendo per iscritto con un sistema, non riesce a distinguere le risposte di una macchina da quelle di un essere umano, allora la macchina ha raggiunto una forma di intelligenza equivalente a quella umana. Questo test — originariamente chiamato test dell'imitazione — continua a essere un punto di riferimento, pur nella sua controversia, nel dibattito sull'intelligenza artificiale (a qualcuno verrà in mente una delle prime scene dello storico film *Blade Runner*).

Durante la Seconda guerra mondiale, Turing fu uno dei protagonisti del progetto Bletchley Park, dove fu costruito il Colossus: il primo computer elettronico "Turing-completo" della storia, impiegato per decifrare le comunicazioni cifrate dei nazisti. La sua esistenza fu tenuta segreta per decenni dai servizi segreti britannici.

3. Il machine learning: quando la macchina impara dagli esempi

3.1 Origini e fondamenti concettuali

L'intelligenza artificiale come campo di ricerca autonomo nacque formalmente nel 1956, in occasione di un workshop organizzato al Dartmouth College da John McCarthy, Marvin Minsky, Claude Shannon e altri pionieri. La proposta di partenza era ambiziosa: la convinzione che ogni aspetto dell'apprendimento e dell'intelligenza potesse essere descritto in modo sufficientemente preciso da essere simulato da una macchina. Quella dichiarazione fondativa conserva ancora oggi tutta la sua forza provocatoria.

Tra le aree che compongono l'intelligenza artificiale, il machine learning — o apprendimento automatico — è quella che negli ultimi decenni ha prodotto i risultati più spettacolari e impattanti. Il suo principio fondamentale è un'inversione rispetto alla programmazione tradizionale: anziché fornire istruzioni esplicite, si forniscono esempi; anziché programmare il comportamento, si addestra il sistema affinché lo scopra autonomamente. La macchina osserva dati, costruisce un modello interno di quei dati e utilizza tale modello per fare previsioni su nuovi casi.

Va precisato, tuttavia, che la programmazione tradizionale non scompare nel machine learning: è essenziale per costruire l'infrastruttura che consente l'addestramento, per definire le architetture

delle reti, per gestire i dati. Il machine learning non sostituisce la programmazione classica; la integra con un nuovo paradigma.

3.2 Le tre famiglie dell'apprendimento automatico

Il machine learning si articola convenzionalmente in tre grandi categorie, che si distinguono per la natura dei dati disponibili e per il tipo di problema da risolvere.

L'apprendimento supervisionato opera su dati etichettati: l'algoritmo riceve coppie di input e output attesi, e impara a generalizzare la relazione tra di essi. Un esempio classico è il riconoscimento delle email di spam: il sistema viene addestrato su migliaia di messaggi già classificati da esseri umani, e impara a distinguere autonomamente i messaggi indesiderati da quelli legittimi. Un altro esempio è il riconoscimento di cifre scritte a mano, applicazione su cui torneremo in dettaglio.

L'apprendimento non supervisionato opera invece su dati privi di etichette. L'algoritmo non riceve indicazioni sull'output atteso, ma deve scoprire autonomamente la struttura latente nei dati. Il clustering, per esempio, raggruppa automaticamente elementi simili senza che sia stata fornita alcuna definizione a priori dei gruppi. Questa tecnica trova applicazione nella segmentazione dei clienti di un'azienda, nell'analisi di pattern comportamentali o nell'individuazione di anomalie in flussi di dati.

L'apprendimento con rinforzo è forse il più affascinante dal punto di vista concettuale, perché si avvicina al modo in cui gli esseri viventi apprendono dall'esperienza. Un agente — l'algoritmo — interagisce con un ambiente, compie azioni e riceve segnali di ricompensa o penalità. Attraverso molte iterazioni, impara a sviluppare strategie che massimizzano le ricompense nel lungo periodo. È questa la tecnica alla base di AlphaGo e dei suoi successori.

La distinzione tra queste categorie non è sempre netta: un problema può essere inquadrato in modi diversi, e spesso i sistemi più efficaci combinano tecniche di categorie diverse.

3.3 MENACE: la macchina di fiammiferi che impara

Un esempio straordinariamente elegante di apprendimento con rinforzo — e particolarmente utile per comprendere intuitivamente il meccanismo — è MENACE (Matchbox Educable Noughts and Crosses Engine), ideato dal matematico Donald Michie negli anni Sessanta del Novecento. MENACE è una macchina puramente analogica, costruita con scatole di fiammiferi, eppure in grado di imparare a giocare a tris in modo sempre più efficace.

Il principio è semplice: ogni possibile configurazione del gioco è rappresentata da una scatola di fiammiferi, al cui interno si trovano gettoni colorati corrispondenti alle possibili mosse. Quando è il turno di MENACE, si estrae casualmente un gettone e si esegue la mossa corrispondente. Alla fine della partita, se MENACE ha vinto, i gettoni utilizzati vengono reinseriti in numero raddoppiato — aumentando la probabilità che quelle mosse vengano scelte in futuro. Se ha perso, i gettoni non vengono reinseriti — diminuendo progressivamente la probabilità di ripetere quella sequenza.

Il risultato è sorprendente: dopo circa venti partite, MENACE riesce già a pareggiare contro un avversario ottimale; dopo duecento, il suo gioco è diventato sostanzialmente ottimale. Nessuno ha programmato le regole della strategia: sono emerse spontaneamente dalla pressione selettiva delle ricompense e delle penalità. MENACE dimostra che il principio del reinforcement learning è profondamente naturale e non richiede, nella sua essenza, nulla di più sofisticato di un meccanismo di feedback.

4. Reti neurali e deep learning: architetture dell'intelligenza artificiale

4.1 Il neurone artificiale e la sua storia

Le reti neurali artificiali hanno radici che risalgono alla prima ricerca sull'intelligenza artificiale. Nel 1943, Warren McCulloch e Walter Pitts proposero un modello matematico del neurone biologico: un'unità che riceve segnali da altri neuroni attraverso connessioni pesate, somma questi segnali e si attiva se la somma supera una certa soglia. Dimostrarono che una rete di tali neuroni era in grado di calcolare qualsiasi funzione logica booleana, e quindi — in linea di principio — di eseguire qualsiasi tipo di computazione.

Il modello è rimasto sostanzialmente invariato nella sua struttura fondamentale. Ogni neurone è caratterizzato da due tipi di parametri: i pesi dei collegamenti con i neuroni precedenti — che determinano l'importanza relativa di ogni segnale in ingresso — e il bias, una soglia individuale che il neurone deve superare per attivarsi. La funzione di attivazione, che trasforma la somma pesata in un segnale di uscita, assume varie forme nelle implementazioni moderne.

La caratteristica cruciale delle reti neurali profonde è la loro organizzazione a strati: i dati entrano dal livello di input, vengono trasformati da uno o più livelli nascosti e producono un risultato al livello di output. Ogni livello apprende a riconoscere caratteristiche progressivamente più astratte: nei sistemi di riconoscimento delle immagini, i primi livelli identificano bordi e variazioni di luminosità, i livelli intermedi compongono questi elementi in forme geometriche, e i livelli più profondi riconoscono concetti di alto livello come «faccia», «automobile» o «cifra».

4.2 Il dataset MNIST e l'addestramento supervisionato

Un caso di studio particolarmente illustrativo è la classificazione delle cifre scritte a mano, un problema che, pur nella sua apparente semplicità, è stato a lungo un banco di prova fondamentale per gli algoritmi di apprendimento automatico. Il dataset MNIST — Modified National Institute of Standards and Technology — raccoglie 70.000 immagini in scala di grigi di cifre scritte a mano da persone di età, professioni e background culturali diversi. Ogni immagine è composta da 784 pixel (28×28) e include una etichetta che indica la cifra rappresentata.

Una rete neurale semplice per questo compito potrebbe avere quattro livelli: il livello di input (784 neuroni, uno per pixel), due livelli nascosti con 16 neuroni ciascuno, e un livello di output con 10 neuroni (uno per ciascuna cifra da 0 a 9). Questa architettura implica circa 13.000 parametri — pesi e bias — che all'inizio assumono valori casuali e vengono progressivamente aggiustati durante l'addestramento.

Il processo di addestramento si articola in due fasi complementari. Nella forward propagation, un'immagine viene presentata alla rete: i valori dei pixel si propagano attraverso i livelli, attivando neuroni in base ai pesi correnti, finché il livello di output produce una previsione. Nella backpropagation, l'errore tra la previsione e la risposta corretta viene quantificato e propagato all'indietro attraverso la rete: ogni peso viene aggiustato in proporzione al suo contributo all'errore

totale. Questo ciclo si ripete per tutte le immagini del dataset — spesso più volte — finché i parametri convergono verso valori che minimizzano l'errore complessivo.

Un aspetto cruciale — e spesso sottovalutato — è la qualità e la rappresentatività del dataset di addestramento. Una rete addestrata su dati omogenei fallirà quando incontrerà input diversi da quelli su cui ha imparato. Questo principio ha implicazioni profonde per le applicazioni reali dell'intelligenza artificiale: un sistema di riconoscimento facciale addestrato principalmente su volti di un certo gruppo demografico tenderà a performare peggio su altri gruppi. La costruzione di dataset rappresentativi è dunque un problema tanto tecnico quanto etico.

4.3 L'evoluzione di AlphaGo: quando la macchina diventa il proprio maestro

La storia delle versioni di AlphaGo illustra in modo particolarmente eloquente la traiettoria del deep learning. La prima versione, che sconfisse nel 2015 il campione europeo Fan Hui, era stata addestrata su milioni di partite giocate da maestri umani — apprendimento supervisionato. Una seconda versione, potenziata dall'autogioco (la macchina giocava partite contro se stessa, imparando da esse), sconfisse nel 2016 Lee Sedol, una leggenda del Go.

AlphaGo Zero rappresentò un salto ulteriore: fu addestrato esclusivamente attraverso l'autogioco, senza alcuna partita umana come punto di partenza. Partendo dalla sola conoscenza delle regole del gioco, sviluppò autonomamente strategie che non solo eguagliarono ma superarono quelle delle versioni precedenti. Il messaggio implicito è potente: il «sapere» umano accumulato in secoli di gioco del Go non era necessario — era anzi un limite. La macchina, libera di esplorare senza pregiudizi, ha scoperto strategie che i maestri umani non avevano mai immaginato.

AlphaZero generalizzò ulteriormente questa capacità a più giochi da tavolo. Addestrato sugli scacchi in nove ore totali, raggiunse il livello del miglior programma scacchistico al mondo — Stockfish, sviluppato nell'arco di oltre tredici anni — in appena quattro ore. Il confronto con la nascita di Deep Blue, che aveva richiesto circa dodici anni di lavoro, è quasi vertiginoso.

5. I large language model (LLM) e la generazione di testo

Nel novembre 2022, il rilascio pubblico di ChatGPT da parte di OpenAI segnò un punto di svolta nella percezione pubblica dell'intelligenza artificiale. ChatGPT si basa su GPT — Generative Pre-trained Transformer — un modello linguistico di grandissime dimensioni addestrato su una quantità enorme di testi provenienti dal web, da libri, da articoli scientifici e da molte altre fonti.

L'architettura Transformer, introdotta nel 2017, è la chiave tecnica di questi sistemi. Si basa su meccanismi di attenzione che consentono al modello di pesare l'importanza relativa di ciascuna parola in un contesto, comprendendo relazioni semantiche complesse indipendentemente dalla distanza nella sequenza. Questa capacità di «leggere» il testo in modo non lineare ha reso i Transformer straordinariamente efficaci nella modellazione del linguaggio naturale.

I modelli linguistici di grandi dimensioni (LLM) non si limitano al testo: le versioni multimodali sono in grado di elaborare immagini, audio e video insieme al linguaggio. Parallelamente, sono emersi modelli generativi specializzati nella creazione di immagini a partire da descrizioni testuali, nella sintesi di video e nella generazione musicale.

È tuttavia essenziale comprendere i limiti fondamentali di questi sistemi. Gli LLM operano su pattern statistici del linguaggio: apprendono quali sequenze di parole sono plausibili in un contesto dato, senza accedere a una comprensione causale o semantica profonda del mondo. Questo li rende capaci di produrre testi persuasivamente coerenti, ma anche di generare affermazioni false con la stessa sicurezza con cui producono quelle vere — il fenomeno delle «allucinazioni».

Un celebre caso del 2023 vide uno studio legale statunitense presentare in tribunale documenti redatti con l'aiuto di ChatGPT che contenevano sei precedenti giurisprudenziali completamente inventati dal modello. Il testo era impeccabilmente strutturato e plausibile nella forma; era semplicemente falso nel contenuto.

Noam Chomsky, tra altri studiosi, ha sottolineato che questi modelli non sono in grado di operare inferenze causali: possono descrivere correlazioni statistiche nel linguaggio, ma non spiegare perché le cose accadono. La critica più incisiva rivolta agli LLM dalla ricerca accademica riguarda proprio la loro assenza di capacità ragionativa genuina: il testo che producono può sembrare il frutto di profonda comprensione, ma è in realtà il risultato di sofisticate interpolazioni statistiche.

Questo approccio metodico si è poi evoluto grazie proprio alle reti neurali e al loro impiego negli LLM.

6. I tre pilastri del successo del deep learning

Una domanda naturale sorge osservando i successi recenti dell'intelligenza artificiale: perché solo ora? Le idee fondamentali delle reti neurali risalgono al 1943, i principi teorici del machine learning sono stati elaborati negli anni Sessanta e Settanta. Cosa ha reso possibile la rivoluzione attuale?

La risposta risiede nella convergenza simultanea di tre fattori:

- **Disponibilità di dati su scala massiva.** L'espansione di Internet e la digitalizzazione pervasiva dell'esperienza umana hanno generato quantità inimmaginabili di dati etichettati e non etichettati. Le reti neurali profonde, per converso, migliorano le proprie prestazioni in modo quasi illimitato all'aumentare dei dati disponibili. «data is the new oil» (tradotto i dati sono il nuovo petrolio) è una formula riduttiva ma efficace per catturare questa dipendenza.
- **Potenza di calcolo.** L'addestramento di reti neurali profonde è computazionalmente intensivo. La svolta è venuta dall'utilizzo delle GPU — originariamente progettate per la grafica dei videogiochi — per l'addestramento parallelo delle reti. La progressiva specializzazione dei chip per l'intelligenza artificiale ha accelerato ulteriormente questa tendenza, riducendo i tempi di addestramento da settimane a ore.
- **Algoritmi efficienti.** Infine, la disponibilità di algoritmi rapidi e stabili per l'ottimizzazione dei parametri — in particolare le varianti dell'algoritmo di backpropagation — ha reso praticabile l'addestramento di reti con miliardi di parametri. È proprio per i contributi fondamentali in questo campo che Geoffrey Hinton e John Hopfield hanno ricevuto il Premio Nobel per la Fisica nel 2024.

La sinergia tra questi tre fattori ha creato un ciclo virtuoso: più dati alimentano reti più grandi, che richiedono più potenza di calcolo, che stimola lo sviluppo di hardware specializzato e algoritmi più efficienti, che a loro volta rendono praticabile l'addestramento su ancora più dati. Il ritmo di questo ciclo ha superato le previsioni più ottimistiche.

7. Applicazioni emblematiche: da AlphaFold a Vista

Il Premio Nobel per la Chimica 2024 è stato riconosciuto ai creatori di AlphaFold2, un'intelligenza artificiale sviluppata da DeepMind capace di prevedere la struttura tridimensionale delle proteine a partire dalla loro sequenza aminoacidica. Questo problema — rimasto irrisolto per cinquant'anni e considerato uno dei grandi problemi aperti della biologia molecolare — è stato affrontato con precisione straordinaria da un sistema di deep learning.

L'impatto scientifico di AlphaFold2 è difficile da sovrastimare: la struttura delle proteine determina la loro funzione, e comprendere questa relazione è fondamentale per lo sviluppo di nuovi farmaci, per la comprensione di malattie genetiche e per la biologia sintetica. In pochi anni, AlphaFold2 ha reso disponibili previsioni strutturali per centinaia di milioni di proteine, accelerando la ricerca in modo che sarebbe stato impensabile con i metodi sperimentali tradizionali.

All'estremo opposto dello spettro applicativo si colloca Vista, un sistema di intelligenza artificiale sviluppato dalla U.S. Air Force per pilotare autonomamente un caccia F-16. Nell'aprile 2024, un aereo a guida autonoma si è confrontato in cielo con piloti umani in un combattimento simulato. La sperimentazione era sufficientemente avanzata da convincere il Segretario dell'aeronautica statunitense a salire a bordo dell'aereo pilotato dall'IA come passeggero, a quasi 900 km/h.

Le implicazioni economiche e strategiche sono immediate: un caccia che non debba ospitare un pilota umano può essere costruito eliminando tutti i sistemi di sopravvivenza necessari in quota e ad alta velocità, riducendo il costo da circa 70 milioni di dollari a un intervallo compreso tra 10 e 20 milioni. Le implicazioni etiche sono altrettanto immediate, e più difficili da affrontare.

AlphaFold2 e Vista rappresentano due poli di un'unica rivoluzione tecnologica: nel primo caso, l'intelligenza artificiale accelera il progresso scientifico in modi che beneficiano l'umanità intera; nel secondo, potenzia capacità militari in modo che potrebbe destabilizzare gli equilibri geopolitici. La tecnologia è la stessa; il suo impatto dipende interamente dalle decisioni umane su come impiegarla.

8. Il lavoro nell'era dell'intelligenza artificiale

La domanda che percorre, talvolta in modo esplicito talvolta implicito, ogni discussione pubblica sull'intelligenza artificiale è: cosa accadrà ai lavoratori umani? È una domanda legittima e urgente, ma beneficia di essere collocata in una prospettiva storica.

Quando VisiCalc — il primo foglio elettronico della storia, sviluppato da Dan Bricklin alla fine degli anni Settanta — fece la sua comparsa, molti analisti prevederono la scomparsa della professione del commercialista. L'argomentazione era apparentemente solida: se una dichiarazione dei redditi è essenzialmente un insieme di calcoli concatenati, e se una macchina può eseguire quei calcoli automaticamente, a cosa serve il commercialista?

Quarantacinque anni dopo, i commercialisti esistono ancora. Ciò che è scomparso è la figura del commercialista che non sa usare il foglio elettronico. La tecnologia non ha eliminato la professione; ha ridefinito le competenze necessarie per esercitarla, elevando il livello minimo di competenza tecnica e liberando il professionista dalle attività di calcolo meccanico per concentrarsi su compiti di analisi, interpretazione e consulenza strategica.

È ragionevole ipotizzare che la dinamica si ripeta con l'intelligenza artificiale. Non sarà l'IA a sostituire il lavoratore umano tout court, ma chi sa utilizzare l'IA efficacemente tenderà a spiazzare chi non lo sa fare. La natura del vantaggio competitivo si sposta: dalla capacità di eseguire calcoli o routine alla capacità di formulare i problemi nel modo giusto, di interpretare criticamente i risultati prodotti dall'IA, di integrare il giudizio umano là dove i pattern statistici non bastano.

Questo non significa che la transizione sarà indolore. Le trasformazioni tecnologiche generano perdenti oltre che vincitori, almeno nel breve e medio periodo, e la velocità attuale del cambiamento rende più difficile l'adattamento. La domanda rilevante non è se l'IA trasformerà il mercato del lavoro — lo trasformerà, irreversibilmente — ma come le istituzioni, i sistemi educativi e le politiche pubbliche possano facilitare questa transizione in modo equo.

9. Machine learning e programmazione tradizionale: una complementarità necessaria

Un equivoco ricorrente nel dibattito pubblico sull'intelligenza artificiale è l'idea che il machine learning abbia reso obsoleta la programmazione tradizionale. La realtà è più sfumata e più interessante.

Il confronto tra AlphaFold2 e AlphaGo/AlphaZero — entrambi prodotti della stessa azienda, DeepMind — illustra bene questa complementarità. Pur condividendo la stessa architettura di base (reti neurali profonde), i due sistemi affrontano problemi completamente diversi con approcci completamente diversi. Non esiste un'unica «intelligenza artificiale» universale: ogni applicazione richiede scelte progettuali specifiche in termini di architettura della rete, strategia di addestramento, qualità dei dati, funzioni di perdita e molti altri parametri.

Inoltre, tutta l'infrastruttura che rende possibile il funzionamento dei sistemi di deep learning — i framework di calcolo distribuito, i sistemi di gestione dei dati, le pipeline di addestramento, le interfacce utente — è costruita con programmazione tradizionale, solida e affidabile. Il machine learning non esiste nel vuoto: è sostenuto da un enorme edificio di codice classico.

Il machine learning offre un nuovo paradigma per la creazione di sistemi: invece di specificare esplicitamente il comportamento desiderato, lo si fa emergere da esempi. In alcuni contesti — quelli in cui le regole sono troppo complesse per essere formalizzate, o in cui i pattern rilevanti cambiano nel tempo — questo approccio è trasformativo. In altri contesti — quelli che richiedono comportamento deterministico, tracciabilità, affidabilità garantita — la programmazione tradizionale rimane insostituibile.

La competenza più preziosa, in questo scenario, è la capacità di identificare quale paradigma sia più appropriato per ciascun problema e di combinare efficacemente i due approcci. Non si tratta di scegliere tra machine learning e programmazione classica: si tratta di sapere quando usare ciascuno strumento.

10. Riflessioni conclusive: potere, responsabilità e futuro

I progressi del machine learning e del deep learning degli ultimi anni sono genuinamente straordinari. La capacità di addestrare sistemi che raggiungono o superano le prestazioni umane in domìni specifici — dal gioco del Go alla previsione della struttura delle proteine, dal riconoscimento facciale alla traduzione automatica — è stata raggiunta con una velocità che ha sorpreso gli stessi ricercatori del settore.

Ma sarebbe un errore confondere le capacità straordinarie con l'intelligenza nel senso pieno del termine. I sistemi di deep learning eccellono in ciò per cui sono stati addestrati; fuori da quel dominio, mostrano fragilità sorprendenti. Non posseggono comprensione causale del mondo, non ragionano in senso genuino, non trasferiscono facilmente il sapere acquisito in un dominio a domini diversi. Le reti neurali profonde sono macchine per l'interpolazione statistica di alta qualità; sono strumenti di potenza enorme, ma strumenti, non agenti intelligenti nel senso filosofico del termine.

Questa distinzione non è accademica: ha implicazioni pratiche immediate. Un sistema medico di diagnosi basato su deep learning che produce una raccomandazione sbagliata non lo fa per «distrazione» o «incomprensione» — lo fa perché il pattern che ha incontrato è sufficientemente diverso da quelli su cui è stato addestrato. Comprendere questo limite è essenziale per progettare sistemi affidabili e per mantenere un controllo umano significativo sulle decisioni ad alto rischio.

Sul piano dell'impatto sociale, l'intelligenza artificiale pone sfide che vanno ben oltre il mondo del lavoro: questioni di privacy e sorveglianza, di responsabilità legale quando un sistema automatizzato causa un danno, di equità quando i dati di addestramento riflettono bias storici, di sicurezza nazionale quando le stesse tecnologie possono potenziare tanto la ricerca medica quanto i sistemi d'arma autonomi.

La storia della tecnologia ci insegna che ogni strumento potente è moralmente neutro: l'uso che se ne fa dipende dalle scelte umane, individuali e collettive. Il fuoco consente di cuocere il cibo e di distruggere foreste; l'energia nucleare alimenta città e costruisce bombe. L'intelligenza artificiale non fa eccezione. La differenza, rispetto ai precedenti storici, è la velocità con cui questa tecnologia si diffonde e la pervasività della sua integrazione in ogni aspetto della vita sociale ed economica.

Questa velocità rende più urgente — non meno — la necessità di istituzioni capaci di governarne lo sviluppo e l'applicazione.

Come ha osservato Edsger Dijkstra: chiedersi se un computer possa pensare è come chiedersi se un sottomarino possa nuotare. La domanda più rilevante non è se la macchina pensa, ma cosa possiamo fare con le sue straordinarie capacità — e cosa dobbiamo preservare come prerogativa esclusivamente umana.

Il machine learning ci ha consegnato un modo radicalmente nuovo di creare sistemi: non programmando il comportamento, ma coltivando l'apprendimento. Questo cambia il tipo di domande che dobbiamo porci come progettisti, come policy-maker, come cittadini. Non più solo «come faccio la macchina a fare X», ma «quali dati devo fornirle», «quali valori voglio che apprenda», «come mi assicuro che ciò che impara corrisponda a ciò che voglio». Sono domande tecniche, ma sono anche domande profondamente umane.

Capitolo 2 – La penetrazione dell'AI nel sistema industriale italiano

1. L'intelligenza artificiale: una tecnologia di sistema

Il dibattito sull'intelligenza artificiale ha raggiunto una pervasività senza precedenti. Convegni, studi, articoli e iniziative istituzionali si moltiplicano con un'intensità proporzionale all'ampiezza — e spesso all'ambiguità — della materia. Questo fermento, però, rischia di oscurare una domanda fondamentale: di cosa si parla esattamente quando si parla di intelligenza artificiale? E quale significato assume, concretamente, la fase attuale per imprese, lavoratori e cittadini?

Una definizione operativa utile descrive l'IA come quell'insieme di sistemi capaci di analizzare il proprio ambiente con un certo grado di autonomia, elaborando azioni orientate al raggiungimento di obiettivi specifici. Questa caratterizzazione, adottata anche dall'OCSE e recepita dall'Unione Europea nell'AI Act del 2024, ha il pregio di essere sufficientemente ampia da includere applicazioni molto diverse tra loro — dagli assistenti vocali ai robot industriali autonomi — pur mantenendo un riferimento chiaro al ruolo delle istruzioni e dei valori umani come quadro di riferimento imprescindibile.

È importante ricordare che l'IA non è un fenomeno recente: come disciplina accademica è insegnata nelle università da oltre settant'anni. Ciò che è cambiato, radicalmente, è la sua rilevanza pratica. Lo sviluppo dell'intelligenza artificiale ha attraversato stagioni alterne — le cosiddette «primavere» e gli «inverni» — con fasi di entusiasmo seguite da delusioni e ridimensionamenti. La terza primavera, quella che stiamo vivendo, si distingue per un elemento cruciale: non è isolata. Si accompagna a una convergenza di progressi tecnologici — nei Big Data, nel cloud computing, nell'High Performance Computing, nelle reti di connettività a banda ultralarga — che crea un effetto di amplificazione reciproca. Il «volano digitale» che ne risulta tende ad autoalimentarsi: la digitalizzazione di un settore accelera l'adozione di nuove tecnologie in settori contigui.

Il catalizzatore simbolico di questa stagione è stato il lancio di ChatGPT nell'autunno del 2022: il primo large language model (LLM) reso accessibile gratuitamente al grande pubblico ha raggiunto cento milioni di utenti in soli due mesi — una velocità di diffusione senza precedenti nella storia

della tecnologia consumer, che mette in prospettiva la traiettoria di Instagram (trenta mesi) e di Spotify (cinquantacinque mesi) per raggiungere lo stesso traguardo.

L'IA non è una singola tecnologia ma una famiglia di tecnologie. Chatbot e modelli linguistici, sistemi di previsione meteo, algoritmi per la ricerca farmacologica: sono tutti «intelligenza artificiale», ma operano su principi, dati e architetture profondamente diversi. Ridurre l'IA a ChatGPT è come ridurre l'elettricità alla lampadina.

Per le imprese, il punto di partenza per qualsiasi strategia di adozione dell'IA è la consapevolezza del proprio patrimonio di dati. I modelli di intelligenza artificiale si alimentano di dati: la loro qualità, quantità e rappresentatività determinano in misura decisiva la qualità dei risultati. Purtroppo, molte organizzazioni — anche di dimensioni rilevanti — non hanno ancora una mappatura chiara dei dati che generano nei propri processi interni e nelle relazioni con clienti e fornitori. Prima di chiedersi "quale IA adottare", è necessario chiedersi "quali dati ho e in quale stato si trovano".

2. La fotografia dell'adozione in Italia

2.1 Il quadro statistico nazionale

I dati ISTAT forniscono la base empirica più affidabile per valutare la diffusione dell'intelligenza artificiale nel sistema produttivo italiano. Il quadro che emerge è articolato e, per certi versi, controintuitivo: il percorso non è stato lineare, e i numeri nascondono divari profondi tra settori, dimensioni aziendali e territori.

Nel 2021, il 6,2% delle imprese italiane con almeno dieci addetti dichiarava di utilizzare almeno una tecnologia di IA. Nel 2023, sorprendentemente, questa quota è scesa al 5%, indicando una fase di rallentamento attribuibile a una combinazione di fattori: costi di implementazione percepiti come eccessivi, carenza di competenze specializzate, incertezza normativa. Poi, nel 2024, la ripresa: l'8,2% delle imprese dichiara di impiegare almeno una tecnologia IA, trainato in particolare dall'industria manifatturiera (8%) e dai servizi non finanziari (9%).

8,2% — delle imprese italiane con ≥10 addetti utilizza almeno una tecnologia IA (2024)

13,5% — la media europea nello stesso anno — un divario di 5,3 punti percentuali

27,6% — il settore telecomunicazioni, quello con la maggiore penetrazione dell'IA in Italia

Nel confronto europeo, l'Italia continua a occupare una posizione di retroguardia. Il divario rispetto alla media UE si è ampliato in termini assoluti — da 2,9 punti percentuali nel 2021 a 5,3 nel 2024 — pur rimanendo sostanzialmente stabile in termini relativi. Paesi come la Danimarca, la Svezia e il Belgio si attestano su livelli di adozione significativamente superiori, mentre l'Italia si colloca nella parte bassa della classifica europea.

2.2 Divari settoriali e dimensionali

Le differenze tra settori sono marcate. Il comparto tessile e della moda registra un utilizzo dell'IA pari al 4,6% delle imprese — ben al di sotto della media nazionale. All'opposto, la fabbricazione di apparecchiature elettroniche raggiunge il 15,7%, e il settore delle telecomunicazioni il 27,6%. Questi dati riflettono non solo la diversa maturità digitale dei settori, ma anche la diversa intensità di dati che caratterizza i rispettivi processi produttivi.

Il divario dimensionale è ancora più pronunciato. Tra le imprese con meno di cinquanta addetti, solo l'1,4% ha implementato tecnologie IA per almeno tre finalità aziendali nel 2023. La quota sale all'8,7% per le imprese con oltre 250 addetti. In un Paese dove le PMI rappresentavano il 99,3% delle imprese attive nel 2022, questo "divide" dimensionale non è un dato marginale: è la principale sfida strutturale per la diffusione dell'IA nel sistema produttivo italiano.

Le principali barriere all'adozione dell'IA rilevate da ISTAT sono i costi elevati (segnalati dal 49,6% delle imprese nel 2023) e la mancanza di competenze digitali adeguate (55,1%). Due ostacoli che si rinforzano reciprocamente: senza competenze, anche gli investimenti tendono a essere meno efficaci.

2.3 Dove si concentra l'uso dell'IA nelle funzioni aziendali

L'analisi ISTAT per funzione aziendale rivela tendenze interessanti nel periodo 2021-2024. L'IA risulta crescentemente strategica per la Ricerca & Sviluppo, per i processi amministrativi e per il marketing e le vendite. Parallelamente, si registra un relativo ridimensionamento nell'uso dell'IA

nei processi di produzione diretta, nella logistica, nella sicurezza ICT e nella contabilità. Queste evidenze, apparentemente controintuitive, suggeriscono che le imprese italiane stiano privilegiando applicazioni di IA nelle funzioni «di supporto» rispetto alle applicazioni nelle funzioni operative core — un pattern che merita analisi più approfondite, anche a livello settoriale e territoriale.

3. Come le imprese italiane usano l'IA: 241 casi concreti

3.1 La mappatura: metodo e dimensioni

Il cuore del report realizzato da Confindustria è una mappatura sistematica di 241 casi d'uso reali, raccolti da 76 aziende italiane che hanno partecipato al Sounding Board Intelligenza Artificiale di Confindustria. Si tratta di applicazioni già attive e operative — non sperimentazioni teoriche o scenari futuri — che restituiscono una fotografia autentica dello stato dell'arte nell'adozione dell'IA nel sistema produttivo nazionale.

La distribuzione per settore riflette la rilevanza strategica attribuita ai diversi verticali: salute e scienze della vita (21,6%), manifatturiero (20,7%), mobilità sostenibile (17,4%), pubblica amministrazione (6,6%), turismo (5,4%), con il 28,2% dei casi applicabili a più settori o non classificabili in un singolo verticale. Per funzione aziendale, le operations rappresentano il 37,3% dei casi, seguite dalle funzioni corporate e HR (12,4%), manutenzione (7,9%), servizio clienti (7,5%), ricerca e sviluppo (7,1%), sales e marketing (6,6%), finanza e acquisti (6,2%) e quality control (3,3%).

Un dato significativo: i casi d'uso basati su IA generativa rappresentano il 18,3% del totale — una quota rilevante ma non dominante. Questo dato segnala che la discussione pubblica, polarizzata attorno ai modelli linguistici, sottorappresenta la vastità e la maturità delle applicazioni di intelligenza artificiale «tradizionale» già profondamente integrate nei processi aziendali.

3.2 Sanità e scienze della vita: la medicina che impara

Il settore sanitario è probabilmente quello dove l'impatto dell'IA sarà più trasformativo nei prossimi anni. Le applicazioni attualmente operative in Italia coprono un arco molto ampio, dalla gestione documentale alla diagnostica avanzata.

Nell'automazione della documentazione clinica, sistemi di trascrizione speech-to-text integrati con modelli linguistici avanzati consentono la generazione automatica di referti medici durante le visite, liberando i professionisti dalla compilazione burocratica e permettendo loro di concentrarsi sull'interazione con il paziente. Nella diagnostica per immagini, algoritmi di deep learning analizzano radiografie, TAC e risonanze magnetiche, identificando anomalie con una precisione e velocità che supera le capacità della revisione manuale — riducendo i falsi negativi e accelerando i percorsi diagnostici.

I sistemi di supporto alle decisioni cliniche rappresentano un'altra frontiera: analizzando cartelle cliniche elettroniche, risultati di laboratorio e letteratura scientifica, l'IA offre suggerimenti personalizzati per diagnosi e terapie, particolarmente utili nei contesti multidisciplinari dove la sintesi rapida di informazioni provenienti da specialità diverse è critica.

La medicina di precisione e la farmacogenomica beneficiano di pipeline bioinformatiche capaci di analizzare gli effetti congiunti di mutazioni multiple, identificando le terapie più appropriate per profili genetici specifici. Questo approccio, impraticabile con i metodi tradizionali per la complessità computazionale richiesta, apre una nuova era nella personalizzazione delle cure oncologiche e nel trattamento delle malattie genetiche rare.

3.3 Manifatturiero: efficienza, previsione, sicurezza

Nel manifatturiero, le applicazioni di IA sono tra le più mature e consolidate. Oltre alla manutenzione predittiva — che rappresenta il caso d'uso più diffuso e sarà trattata in dettaglio nella sezione dedicata — spiccano alcune applicazioni particolarmente innovative.

I gemelli digitali (digital twin) — repliche virtuali precise di impianti fisici — permettono di monitorare le performance in tempo reale, simulare scenari, ottimizzare i consumi energetici e

pianificare gli interventi con un livello di granularità impossibile da raggiungere con metodi tradizionali. In alcuni casi, il gemello digitale si concentra su un singolo macchinario; in altri, modella l'intero stabilimento o la catena logistica.

Sistemi di computer vision integrati nell'automazione industriale consentono il riconoscimento di oggetti in scene non strutturate e caotiche — estendendo le capacità dei robot industriali a compiti precedentemente impossibili da automatizzare. Nel campo della gestione del magazzino, la computer vision automatizza il riconoscimento e la tracciabilità dei materiali, superando i limiti dei sistemi basati su etichette fisiche soggette a deterioramento.

Particolarmente innovativa è l'applicazione dell'IA alla previsione dei costi di produzione per nuovi prodotti: attraverso l'analisi di database storici, i sistemi stimano in pochi secondi i costi di realizzazione di prodotti mai realizzati prima, riducendo i tempi di risposta ai preventivi da ore a secondi e fornendo stime corredate da quantificazione dell'incertezza. In alcuni contesti, questa capacità predittiva si estende al calcolo dell'impronta di CO_2 del prodotto.

3.4 Mobilità sostenibile: ottimizzare per decarbonizzare

Nel settore della mobilità e dei trasporti, l'IA sta accelerando la transizione ecologica oltre a migliorare l'efficienza operativa. Le applicazioni più significative documentate nei casi italiani includono la manutenzione predittiva delle flotte, l'ottimizzazione dei percorsi e la gestione intelligente delle infrastrutture.

Nel trasporto pubblico, algoritmi di manutenzione predittiva misurano il rischio di guasto dei componenti di autobus e sistemi di bordo, consentendo una programmazione proattiva degli interventi che riduce il fermo mezzi, ottimizza le scorte di ricambio e previene interruzioni del servizio. Sistemi analoghi ottimizzano la «curva chilometrica» dei veicoli, raccomandando l'impiego dei mezzi in modo da massimizzare l'utilizzo dei contratti di assistenza e prolungare la vita dei motori.

Nella logistica urbana, algoritmi di ottimizzazione dei percorsi con vincoli multipli — condizioni di traffico, orari, aree di distribuzione, livelli di servizio — hanno consentito riduzioni fino al 25% dei chilometri percorsi, con impatti diretti su consumi ed emissioni. A livello internazionale,

esperienze come quella di un grande operatore logistico statunitense documentano risparmi nell'ordine di 100 milioni di miglia annue e 10 milioni di galloni di carburante grazie all'ottimizzazione IA dei percorsi.

Le esperienze internazionali offrono ulteriori indicazioni: a Londra, algoritmi predittivi sulla rete metropolitana hanno ridotto del 58% le ore di disservizio; in Germania, sistemi predittivi hanno abbattuto del 25% i costi di manutenzione ferroviaria; in Cina, l'ottimizzazione di una flotta di oltre 16.000 autobus elettrici ha ridotto i costi energetici del 43%, evitando 1,35 milioni di tonnellate di CO_2 all'anno.

3.5 Pubblica amministrazione: la città intelligente

La pubblica amministrazione rappresenta uno degli ambiti dove l'impatto dell'IA può essere più diffuso socialmente, pur non essendo sempre il settore dove la trasformazione avviene più rapidamente. I casi italiani documentano applicazioni che spaziano dalla gestione delle infrastrutture urbane al monitoraggio degli spazi naturali.

Sistemi di gestione intelligente dell'illuminazione stradale e delle gallerie integrano sonde IoT con algoritmi di ottimizzazione per adattare automaticamente i livelli luminosi alle condizioni reali, migliorando la sicurezza e riducendo i consumi energetici. Piattaforme di supporto decisionale che integrano big data geografici permettono alle amministrazioni locali di misurare fenomeni urbani complessi — mobilità, qualità dell'aria, flussi commerciali — e simulare l'impatto di diverse politiche prima della loro implementazione.

Nel monitoraggio di grandi spazi naturali e marittimi, sistemi di videosorveglianza potenziati dall'IA applicano algoritmi di scansione rapida ad alta risoluzione per identificare automaticamente situazioni anomale — imbarcazioni in difficoltà, naufraghi, oggetti sospetti — su vaste superfici e in tempi incompatibili con il controllo manuale. Nella gestione dei rifiuti, soluzioni IA integrate con sensoristica IoT hanno ridotto del 50% i giorni di fermo degli impianti di smaltimento.

3.6 Turismo: personalizzazione e gestione dei flussi

Il settore turistico italiano — uno dei più rilevanti per l'economia nazionale — presenta un potenziale ancora largamente inespresso nell'adozione dell'IA. Le stime del Ministero del Turismo indicano che l'IA potrebbe ridurre la concentrazione estiva dei flussi fino al 15%, abbattere i costi operativi fino al 20% e alleggerire del 20% le pressioni sulle aree sovraffollate.

Le applicazioni documentate includono sistemi di dynamic pricing che analizzano in tempo reale domanda, disponibilità, stagionalità e comportamento della concorrenza per ottimizzare le tariffe alberghiere. Strumenti di analisi del sentiment e dei comportamenti di consumo, basati sull'elaborazione di milioni di contenuti online, permettono di comprendere le preferenze dei visitatori con un livello di granularità impossibile con i metodi tradizionali. Soluzioni di IA generativa assistono le strutture ricettive nella gestione delle recensioni, nel supporto alle prenotazioni e nell'interazione con i clienti attraverso chatbot avanzati multilingua disponibili 24/7.

4. Nel cuore delle aziende: un atlante delle funzioni aziendali

4.1 Risorse umane e funzioni amministrative

L'adozione dell'IA nelle funzioni di HR e amministrazione produce effetti a cascata sull'intera organizzazione. I sistemi di analisi organizzativa costruiscono «mappe di competenza» multidimensionali che identificano pattern nascosti nelle dinamiche dei team, supportando decisioni di sviluppo del personale basate su evidenze piuttosto che su intuizioni. Nei processi di selezione, l'automazione dell'analisi dei curricula e l'anonimizzazione dei dati sensibili permettono una valutazione più oggettiva e veloce delle candidature — a condizione che i sistemi siano progettati per controllare i bias presenti nei dati di addestramento, che altrimenti rischiano di replicare pregiudizi storici.

Sul fronte amministrativo, algoritmi di Natural Language Processing automatizzano l'estrazione di informazioni da documenti, fatture e contratti, riducendo i tempi di elaborazione e il rischio di errori. Sistemi di smistamento intelligente delle comunicazioni in arrivo assegnano priorità, indirizzano ai team competenti e generano bozze di risposta — liberando risorse per attività a

maggior valore aggiunto. Nelle funzioni legali, l'IA velocizza la revisione documentale, identifica clausole rilevanti e scadenze, e monitora gli aggiornamenti normativi in modo proattivo, semplificando la compliance aziendale.

Questa trasformazione sta generando nuovi profili professionali all'intersezione tra HR, tecnologia e analisi dei dati — figure ibride che combinano comprensione dei processi organizzativi e capacità di gestire sistemi di IA avanzati. Il futuro delle funzioni amministrative e HR sarà caratterizzato da una crescente sinergia tra automazione intelligente e giudizio umano, secondo una logica di complementarità piuttosto che di sostituzione.

4.2 Manutenzione predittiva: dal calendario al dato

La manutenzione predittiva è tra gli ambiti più maturi nell'adozione dell'IA industriale. Il cambio di paradigma è radicale: si passa dalla manutenzione programmata su calendario — che interviene indipendentemente dallo stato effettivo delle macchine — a interventi basati su dati reali, che anticipano il guasto prima che si manifesti. I benefici documentati includono riduzione del fermo impianti, ottimizzazione delle scorte di ricambio, miglioramento della sicurezza degli operatori e riduzione dei costi operativi complessivi.

Dashboard in tempo reale trasformano il modo in cui gli operatori interagiscono con i sistemi: la disponibilità immediata di diagnostica completa riduce i tempi di risposta agli alert e consente un'allocazione ottimale delle risorse manutentive. Il «meta-monitoraggio» dei sensori stessi — modelli di machine learning che controllano la qualità e l'affidabilità della sensoristica — aggiunge un ulteriore livello di sicurezza al sistema predittivo.

Le applicazioni si estendono ben oltre il manifatturiero: nel trasporto pubblico, nelle infrastrutture stradali e nelle reti elettriche, algoritmi di object detection e computer vision analizzano migliaia di immagini per identificare precocemente formazione di crepe, anomalie strutturali e deterioramenti. Nelle reti idriche e del gas, sistemi di sensoristica IoT integrati con digital twin permettono un monitoraggio continuo e una pianificazione accurata degli interventi, riducendo le perdite e prevenendo guasti critici.

4.3 Servizio clienti: l'assistenza che non dorme mai

Il servizio clienti è uno degli ambiti dove l'IA ha già prodotto trasformazioni più visibili. I chatbot di nuova generazione — alimentati da modelli linguistici avanzati e integrati con i sistemi documentali dell'organizzazione — gestiscono autonomamente le richieste standard, delegano i casi complessi agli operatori più adatti e mantengono un dialogo naturale e contestualizzato. In alcuni contesti specifici, questa automazione ha raggiunto il 100% per determinati servizi, con una drastica riduzione delle chiamate al supporto tradizionale.

L'integrazione omnicanale è un elemento chiave: gli assistenti virtuali gestiscono richieste provenienti da chatbot web, app mobile, canali social e telefonia, identificando automaticamente la natura e l'urgenza delle richieste e instradandole appropriatamente. Sistemi di monitoraggio continuo del sentiment analizzano in tempo reale i feedback su tutti i canali, consentendo all'organizzazione di identificare rapidamente criticità emergenti e adattare i propri servizi. Il vantaggio competitivo risiede nella disponibilità 24/7 e nella capacità di apprendimento continuo: questi sistemi non sono strumenti statici, ma ecosistemi che evolvono insieme all'organizzazione.

4.4 Ricerca e sviluppo: l'accelerazione della scoperta

In nessun ambito il potenziale trasformativo dell'IA è più evidente che nella ricerca e sviluppo. Nel settore farmaceutico, pipeline di analisi bioinformatica permettono di studiare reti biologiche complesse — i pathways mutati nell'oncologia, le interazioni molecolari nelle malattie genetiche rare — con una profondità e velocità impensabili con metodi tradizionali. Piattaforme integrate che combinano IA, simulazioni di dinamica molecolare e chimica quantistica hanno accelerato lo sviluppo di nuovi farmaci candidati, portando due potenziali molecole in fase di sperimentazione clinica in tempi significativamente ridotti.

I digital twin farmaceutici — repliche digitali di entità fisiche integrate con IA predittiva — consentono di simulare gli effetti dei farmaci e virtualizzare parzialmente i test clinici, accelerando i tempi di sviluppo. Nella medicina di precisione, l'IA analizza enormi dataset di dati clinici e genomici per identificare quali pazienti rispondono meglio a terapie specifiche, affrontando il

problema della resistenza terapeutica con un approccio basato su evidenze molecolari piuttosto che su generalizzazioni statistiche.

Fuori dalla farmaceutica, l'IA supporta la ricerca orientata all'ottimizzazione dei processi industriali: sistemi di tracciamento strategico delle emissioni di CO_2, strumenti di machine learning per simulare proprietà di nuove molecole, «copiloti» basati su IA generativa che facilitano il trasferimento di conoscenze tecniche e riducono i tempi di inattività operativa.

4.5 Sales, marketing e finanza: dalla previsione alla personalizzazione

Nel marketing e nelle vendite, l'IA introduce capacità analitiche su dati non convenzionali: sistemi di NLP e computer vision elaborano milioni di contenuti social e immagini online per mappare le reali esperienze di consumo, comprendere contesti d'uso e identificare tendenze emergenti prima che siano rilevabili con i metodi tradizionali. Strumenti di previsione delle vendite basati su IA elaborano segnali interni ed esterni per ottimizzare dinamicamente i riassortimenti di stock, con miglioramenti dell'accuratezza previsionale documentati fino al 19% rispetto ai metodi tradizionali.

Il copywriting assistito dall'IA consente di generare contenuti personalizzati per canali e target diversi, mantenendo la coerenza del messaggio ma adattandone il tono e il registro. In un caso documentato nel settore farmaceutico, l'adozione di questi strumenti ha ridotto del 50% i tempi di produzione dei contenuti e del 70% i costi di copywriting, mantenendo elevati standard qualitativi grazie alla supervisione umana.

Nelle funzioni finanziarie e negli acquisti, l'IA migliora l'analisi del rischio creditizio, automatizza la gestione documentale dei contratti e ottimizza i processi di approvvigionamento. Sistemi di machine learning prevedono la domanda di energia, materie prime e combustibili, integrando dati storici e tendenze di mercato per ottimizzare gli ordini. In casi avanzati, la maturità di questi sistemi è tale da consentire l'automazione parziale o totale di processi come le aste per il rifornimento di carburante.

4.6 Controllo qualità: l'occhio che non si stanca

Il controllo qualità basato su computer vision potenziata dall'IA è uno degli ambiti dove il salto di prestazione rispetto ai metodi tradizionali è più netto. Sistemi di visione artificiale analizzano in tempo reale centinaia di immagini al secondo, verificando la presenza di difetti, controllando l'allineamento dei componenti e valutando la qualità delle finiture superficiali — con una costanza e un'attenzione impossibili da mantenere nel controllo manuale prolungato.

Reti neurali addestrate su migliaia di immagini di prodotti conformi e difettosi identificano anomalie quali errori di assemblaggio, difetti superficiali e componenti mancanti con tassi di rilevamento superiori all'ispezione umana. Nei semiconduttori, algoritmi di deep learning analizzano i wafer per identificare pattern di difetti; nel farmaceutico, sistemi dedicati verificano il corretto riempimento di fiale e l'integrità dei blister; nel manifatturiero generale, la computer vision controlla la presenza e il posizionamento corretto di simboli e componenti.

È importante sottolineare che l'IA in questo ambito non sostituisce gli operatori di qualità: li affianca, occupandosi delle verifiche ripetitive e standardizzate, mentre gli operatori si concentrano sull'analisi delle cause dei difetti e sull'ottimizzazione dei processi — attività che richiedono giudizio contestuale e creatività tecnica.

4.7 IA per la sostenibilità: efficienza come responsabilità

Trasversalmente a tutti i settori, l'IA offre un contributo significativo agli obiettivi di sostenibilità ambientale. Nel settore energetico, sistemi predittivi rilevano precocemente guasti di rete, ottimizzano il bilanciamento tra produzione e consumo e migliorano la previsione della domanda di gas e elettricità, integrando variabili meteorologiche, storici di consumo e previsioni termoelettriche. Soluzioni di auto-scaling basate sull'IA ottimizzano l'utilizzo delle risorse computazionali cloud, riducendo i consumi energetici dei data center.

Nell'agricoltura, sistemi di pianificazione dell'irrigazione che stimano il fabbisogno idrico fino a cinque giorni prima — sulla base di fasi fenologiche delle colture, composizione del suolo e condizioni climatiche — consentono risparmi idrici significativi e migliorano la qualità e la quantità del raccolto. Nelle reti di distribuzione del gas, robot quadrupedi dotati di sensori

monitorano autonomamente manometri, rilevano perdite e sorvegliano gli impianti. Nelle reti idriche, digital twin integrati con IoT permettono simulazioni e pianificazione accurata degli interventi. Nel teleriscaldamento, ensemble di modelli IA che integrano dati meteorologici e serie storiche della domanda energetica riducono gli sprechi e le emissioni di CO_2.

5. La penetrazione settoriale: dove l'AI sta già cambiando la produzione

Al di là dei dati aggregati, l'immagine più fedele della trasformazione in corso emerge dall'analisi settore per settore. La penetrazione dell'AI nell'industria italiana non avviene in modo omogeneo: si concentra nelle filiere con maggiore maturità infrastrutturale digitale, nelle grandi imprese con capacità di investimento e nei segmenti in cui il ritorno economico dell'automazione è più misurabile e più rapido.

5.1 Automazione industriale e manifattura avanzata: la Physical AI entra in fabbrica

Il settore dell'automazione industriale è quello in cui la convergenza tra intelligenza artificiale e sistemi fisici — la cosiddetta Physical AI — ha raggiunto la maturità applicativa più avanzata. Secondo i dati dell'Osservatorio Innovative Robotics del Politecnico di Milano, presentati nel giugno 2026, il 28% delle imprese italiane utilizza già soluzioni robotiche, quota destinata a salire al 36% entro il 2028. Il mercato italiano della robotica ha raggiunto i 3,5 miliardi di euro, con una composizione che si sta rapidamente spostando verso sistemi dotati di capacità autonome e adattive.

Tra le imprese che prevedono investimenti nel 2026, il 29% punta su robot "intelligenti" — sistemi che integrano algoritmi di apprendimento automatico, capacità percettive e aggiornamento continuo dei modelli — con una spesa media prevista di circa 183.000 euro per impresa. I robot collaborativi (cobot), oggi presenti nel 25% delle aziende manifatturiere dotate di automazione, sono attesi al 34% entro il 2028; i robot mobili autonomi (AMR) passeranno dal 24% al 30%; mentre gli umanoidi, oggi in sperimentazione nel 3% delle aziende, potrebbero raggiungere l'11% entro il 2028.

Il paradigma che guida questa evoluzione è passato dall'hardware al software: non si tratta più soltanto di velocizzare le linee o di aumentare la precisione meccanica, ma di costruire sistemi in

grado di apprendere dai dati di processo, adattarsi ai cambi di formato senza programmazione manuale e dialogare in linguaggio naturale con gli operatori. A SPS Italia 2026 il filo conduttore era proprio la Physical AI come infrastruttura cognitiva della fabbrica autonoma, con dimostrazioni operative di sistemi come l'Eigen Engineering Agent di Siemens (agente di IA generativa integrato direttamente nell'ambiente di programmazione PLC) e soluzioni di addestramento di reti neurali su dati di processo senza competenze di data science.

5.2 Farmaceutico: dall'ottimizzazione di processo alla drug discovery

Il settore farmaceutico italiano — che occupa direttamente oltre 67.000 persone, investe circa 1,7 miliardi di euro l'anno in R&S e rappresenta il comparto manifatturiero con il più alto tasso di investimento digitale, superiore del 150% alla media della manifattura nazionale (dati Farmindustria) — è anche quello in cui la penetrazione dell'AI presenta la maggiore eterogeneità applicativa: dal controllo di processo in ottica GMP all'accelerazione della pipeline di ricerca.

Sul versante produttivo, il 2026 ha segnato il passaggio dall'adozione sperimentale all'integrazione strutturale dell'AI nelle linee di produzione farmaceutica, con applicazioni in quattro aree principali: quality control in real-time tramite computer vision e spettroscopia, manutenzione predittiva degli impianti, ottimizzazione dei parametri di processo nelle fasi di miscelazione e confezionamento, e supply chain planning con modelli predittivi per la gestione delle materie prime critiche. Secondo le stime di ZS Associates riferite al mercato globale, l'AI applicata alla fase pre-clinica e di sviluppo iniziale del farmaco potrebbe aumentare il tasso di successo in Phase 1 del 40-50% e ridurre le timeline iniziali nella stessa misura, comprimendo i costi di sviluppo di miliardi di dollari per singola molecola. Il riferimento più emblematico in questo senso è il caso di Insilico Medicine, il cui candidato farmaco contro la fibrosi polmonare idiopatica progettato interamente con IA ha raggiunto la Phase IIa in 18 mesi a un costo stimato di 6 milioni di dollari, contro i 100-200 milioni e i 6-8 anni del percorso tradizionale.

Per l'Italia, che ospita il secondo polo farmaceutico europeo per volumi produttivi dopo la Germania, la sfida è duplice: da un lato, adeguare le infrastrutture digitali degli stabilimenti produttivi ai requisiti di validazione GMP richiesti dagli enti regolatori per i sistemi basati su AI; dall'altro, posizionarsi nella catena globale della ricerca accelerata dall'AI, attraendo investimenti

nella fase di sviluppo computazionale. Su questo secondo fronte, si registra ancora un ritardo rispetto ai cluster anglosassoni e al polo elvetico-tedesco, ma alcune piattaforme di ricerca computazionale sviluppate in collaborazione tra università italiane e industria farmaceutica stanno iniziando a produrre risultati riconoscibili a livello internazionale.

5.3 Food & Beverage e industria alimentare: dalla previsione della domanda alla filiera tracciabile

L'industria alimentare italiana è strutturalmente uno dei terreni più fertili per l'applicazione dell'IA: volumi enormi di dati operativi non strutturati, processi ripetitivi ad alta variabilità stagionale, filiere complesse che integrano agricoltura, trasformazione, distribuzione e retail, vincoli normativi stringenti che premiano la tracciabilità automatica. Secondo il Rapporto 2026 sull'agrifood tech italiano, presentato alla Camera dei Deputati da Federalimentare e Confagricoltura, sono state mappate 573 startup attive nel comparto, con investimenti cresciuti a 122 milioni di euro nel 2025 (+18% rispetto all'anno precedente). Le startup sono classificate in tre categorie: quelle che integrano l'AI nella propria offerta in modo trasversale, quelle che la utilizzano come leva operativa interna, e quelle che l'hanno resa il cuore del proprio modello di business.

A livello di grandi imprese, AlixPartners ha documentato — in occasione del Food Summit 2026, tenutosi a Villa Borromeo nel maggio 2026 — che tra il 2021 e il 2025 i valori del comparto Food & Beverage italiano sono cresciuti a un CAGR di circa il 6%, mentre i volumi hanno registrato una variazione negativa dell'1%, evidenziando una crescita trainata dal valore e non dai volumi. In questo contesto, l'AI applicata alla previsione della domanda per SKU granulare, alla gestione dinamica dei prezzi e all'ottimizzazione delle promozioni commerciali è diventata un differenziatore competitivo riconoscibile. Le grandi imprese alimentari italiane hanno avviato investimenti AI significativi tra il 2023 e il 2025, con budget compresi tra 8 e 35 milioni di euro per i gruppi più strutturati, destinati principalmente alla pianificazione della produzione, al controllo qualità e alla riduzione degli sprechi.

McKinsey ha stimato che gli operatori food che integrano l'AI strutturalmente lungo la pipeline operativa raggiungono guadagni di produttività compresi tra il 12 e il 25%, riduzioni degli sprechi tra il 20 e il 40%, e miglioramenti nei tempi di lancio di nuovi prodotti tra il 30 e il 50%. In Italia, casi documentati includono un distributore di prodotti freschi che serve oltre 4.200 punti vendita

e ha ridotto del 19% i chilometri percorsi dalla flotta refrigerata grazie a un sistema di route optimization AI, e una catena di pasticcerie regionali che ha ridotto del 31% gli invenduti e aumentato le vendite per punto vendita del 9% attraverso modelli di previsione della domanda calibrati su 18 mesi di dati storici.

5.4 Packaging: la qualità si vede in tempo reale

Il settore italiano delle macchine per il packaging — che secondo i preconsuntivi UCIMA ha chiuso il 2025 con un fatturato di 10,2 miliardi di euro (+2,1% sul 2024), con le esportazioni a coprire circa l'80% del totale — sta attraversando una trasformazione in cui l'AI non è più un'opzione ma una condizione di competitività. Le applicazioni di computer vision e machine learning stanno ridefinendo gli standard del controllo qualità in linea, sostituendo o affiancando i sistemi di ispezione tradizionali con soluzioni capaci di rilevare in tempo reale difetti di stampa, anomalie di chiusura, errori di etichettatura e non conformità dei materiali a velocità di linea che rendono impossibile il controllo manuale.

Antares Vision Group — player italiano di riferimento a livello globale nella tracciabilità e nel controllo qualità — ha presentato a Metpack 2026 (Essen, maggio 2026) soluzioni integrate di ispezione AI per lattine e contenitori rigidi destinati al food, al beverage e all'aerosol, con sistemi che combinano telecamere ad alta risoluzione, sensori multipli e algoritmi di deep learning per il rilevamento di anomalie anche minime nelle saldature, nelle bordature e nelle decorazioni di stampa. L'architettura tecnica di questi sistemi — telecamere 2D/3D, illuminazione controllata, reti neurali convoluzionali, integrazione con i sistemi MES di fabbrica — rappresenta oggi lo standard di fatto per le linee di packaging ad alta velocità nei settori alimentare e farmaceutico. Anche all'interno dell'Associazione AIdAM diversi Associati del gruppo visione artificiale dispongono di tecnologie e prodotti non solo per l'inspection ma per il completo addestramento dei robot ai task richiesti nelle diverse industrie.

Un indicatore della direzione di mercato: secondo le proiezioni disponibili, il mercato globale della machine vision raggiungerà i 25 miliardi di dollari entro il 2030, con il packaging tra i settori di crescita più rapida accanto all'automotive e alla farmaceutica. Per il packaging di macchine Made in Italy, che compete sui mercati internazionali sulla base della qualità e dell'affidabilità dei

processi, l'integrazione nativa dell'AI nei sistemi di ispezione e di controllo processo è diventata un requisito implicito nei capitolati tecnici dei principali acquirenti internazionali.

5.5 Logistica e supply chain: la transizione da settore tradizionale a infrastruttura intelligente

La logistica italiana vale circa il 9% del PIL nazionale, occupa oltre 1,4 milioni di addetti e coinvolge circa 79.000 imprese tra trasporto, magazzinaggio e servizi integrati. Il mercato conto terzi ha raggiunto nel 2025 i 112,4 miliardi di euro (+1,9% nominale) e l'Osservatorio Contract Logistics "Gino Marchet" del Politecnico di Milano stimava per il 2026 un superamento della soglia dei 117 miliardi — obiettivo la cui raggiungibilità dipenderà in misura crescente dalla capacità del settore di accelerare sull'innovazione.

Secondo la ricerca dell'Osservatorio Contract Logistics presentata nel febbraio 2026, il 30% delle aziende italiane committenti ha già avviato almeno un progetto di AI nella logistica, con un'adozione prevista al 44% nei prossimi tre anni. L'81% delle aziende che ha adottato soluzioni AI nella logistica riporta benefici tangibili, con una soddisfazione media di 7,7 su 10. Le applicazioni più diffuse riguardano la previsione della domanda e la pianificazione degli ordini, l'ottimizzazione dei percorsi di picking in magazzino, il routing dinamico delle flotte di trasporto e la manutenzione predittiva dei veicoli e delle attrezzature di movimentazione.

Il quadro d'insieme è tuttavia caratterizzato da una forte asimmetria, questa volta non tanto dimensionale quanto culturale. Secondo il Radar IA del Centro sulla Logistica e la Supply Chain (i-LOG) dell'Università Cattaneo – LIUC, condotto su un campione di mille rispondenti, il 71% delle aziende italiane non dispone ancora di AI a supporto dei processi di supply chain e logistica, e il 43% si dichiara scettico rispetto all'investimento nei prossimi 24 mesi. Le barriere citate sono principalmente tre: il divario di competenze interne, i costi iniziali di implementazione percepiti come elevati e l'incertezza sul ritorno dell'investimento. Una struttura di ostacoli sostanzialmente identica a quella rilevata nelle PMI manifatturiere, che suggerisce come il ritardo nell'adozione dell'AI sia un fenomeno trasversale al tessuto produttivo italiano, più culturale e organizzativo che strettamente tecnologico o finanziario.

Sul fronte dell'innovazione emergente, la logistica italiana sta adottando da tempo i sistemi AMR (robot mobili autonomi) per la movimentazione interna di magazzino e le soluzioni di

ottimizzazione dell'intralogistica basate su digital twin, che consentono di simulare e ottimizzare i flussi di magazzino prima di modificare l'assetto fisico degli impianti. Queste tecnologie non solo rendono più efficienti le movimentazioni interne ma finiscono per ottimizzare i processi logistici e migliorare i tempi di consegna finale dei prodotti finiti. Sicuramente sistemi intelligenti di gestione autonoma dei robot mobili renderanno ancora più ottimale il loro impiego.

5.6 Lettura trasversale: cosa accomuna i settori che avanzano

Dall'analisi settoriale emerge un pattern ricorrente che trascende le specificità di ciascuna filiera. I settori e le imprese che stanno realizzando le integrazioni di AI più mature condividono alcune caratteristiche strutturali: una base di dati operativi già raccolta e parzialmente strutturata (IoT, sensori, ERP), una cultura della misurazione dei processi radicata nel tempo, e la capacità di quantificare il ritorno dell'investimento su metriche operative precise (riduzione degli scarti, abbattimento dei fermi macchina, ottimizzazione dei percorsi di consegna).

In tutti i settori analizzati, la frattura più netta non è quella tra settori diversi ma quella tra grande impresa e PMI all'interno dello stesso settore. Le grandi imprese alimentari, farmaceutiche, logistiche e manifatturiere hanno ormai team interni dedicati all'AI e investono in modo sistematico; le PMI degli stessi settori restano prevalentemente escluse, con l'eccezione parziale di chi può accedere a soluzioni verticali pre-configurate (il SaaS per la previsione della domanda nel food, i sistemi di visione AI venduti come moduli integrabili nelle macchine packaging) che abbassano la soglia di accesso senza richiedere competenze di data science interne.

Infine, un elemento trasversale riguarda il profilo del rischio percepito. In settori come il farmaceutico e il food, dove la conformità normativa è un requisito non negoziabile, l'integrazione dell'AI introduce una complessità aggiuntiva legata alla validazione dei sistemi e alla documentabilità delle decisioni algoritmiche — temi che l'AI Act europeo, entrato in vigore nella sua prima fase operativa il 2 agosto 2026, renderà gradualmente obbligatori per i sistemi classificati ad alto rischio. La compliance normativa sull'AI diventa così, per il sistema industriale italiano, non solo una questione di accesso al mercato europeo, ma una precondizione per la piena realizzazione del potenziale trasformativo di queste tecnologie.

6. Cinque lezioni dall'esperienza delle imprese

L'analisi dei 241 casi d'uso prima riportata ha prodotto cinque indicazioni operative che sintetizzano le lezioni apprese dai pionieri dell'adozione dell'IA nel sistema produttivo italiano. Non si tratta di prescrizioni universali, ma di orientamenti emersi dall'esperienza concreta.

Prima lezione: la qualità dei dati è il presupposto di tutto

Nessun algoritmo, per quanto sofisticato, può compensare dati di scarsa qualità. La prima priorità per qualsiasi impresa che intenda adottare sistemi di IA è la costruzione di dataset rappresentativi, accurati e ben strutturati. Questo richiede che gli uffici tecnici interni comprendano l'importanza di alimentare i dataset in modo sistematico e continuativo — non come operazione una tantum, ma come processo permanente. Sia i dati interni che quelli esterni devono essere adeguatamente «puliti» e categorizzati. L'adozione di una data platform dedicata può facilitare questo processo. Il passaggio a un modello aziendale data-driven richiede investimenti in formazione del personale che spesso vengono sottovalutati.

Seconda lezione: il cambiamento è prima di tutto culturale

I risultati migliori si ottengono quando l'IA viene integrata nei processi esistenti con una chiara strategia e un adeguato piano di change management — non quando viene «calata dall'alto» come soluzione miracolosa. Il coinvolgimento del personale fin dalle prime fasi del progetto è determinante: le resistenze ideologiche verso l'IA si superano più facilmente con la partecipazione diretta che con la comunicazione unidirezionale. I manager svolgono un ruolo cruciale nel contestualizzare gli strumenti e nel supportare i team nella transizione. I percorsi di upskilling e reskilling non sono opzionali: sono la condizione necessaria perché l'introduzione dell'IA produca i benefici attesi.

Terza lezione: la tecnologia da sola non basta

L'implementazione di sistemi di IA richiede una struttura tecnica adeguata fin dall'inizio: piattaforme di digitalizzazione, sistemi IoT, infrastrutture di gestione dei dati. Lo sviluppo tramite un team interno è un'opzione valida per costruire competenze riutilizzabili su progetti futuri — ma deve essere accompagnato dalla collaborazione con esperti esterni e startup innovative specializzate. Un risultato inatteso documentato in diversi casi: l'implementazione di IA ha spesso

richiesto una maggiore standardizzazione dei processi e della documentazione interna, producendo benefici organizzativi che vanno oltre l'applicazione specifica.

Quarta lezione: partire in piccolo, imparare in fretta

Le esperienze concrete suggeriscono di privilegiare progetti pilota ben definiti e circoscritti, con valutazione attenta del rapporto costi/benefici a partire da business case pratici. Alcuni esperti sconsigliano, come primo approccio, di avviare progetti con lunghi tempi di sviluppo; preferibile invece un approccio agile basato su rapida prototipazione e iterazione. Va tenuto presente che i benefici dei sistemi di IA possono non essere immediatamente evidenti: alcune applicazioni richiedono tempo e successive versioni per «emergere» il valore per l'impresa. La pazienza strategica è una virtù nell'implementazione dell'IA.

Quinta lezione: l'umano al centro, sempre

L'indicazione più ricorrente, e forse la più importante, riguarda il modello di «intelligenza sorvegliata»: l'IA produce i risultati più significativi quando non è lasciata a sé stessa, ma è costantemente gestita e supervisionata dagli esseri umani. Anche nei processi interamente automatizzati, i lavoratori mantengono il ruolo di monitorare l'efficacia del sistema e il raggiungimento degli obiettivi aziendali. Lungi dall'essere un vincolo, questa supervisione è una garanzia: le risorse umane liberate dall'automazione vengono tipicamente dedicate ad attività a maggior valore aggiunto, con effetti positivi sia sulla produttività che sulla qualità del lavoro.

7. Il quadro normativo europeo: l'AI Act e i suoi effetti

7.1 Il contesto: la regolazione come risposta alla trasformazione

Ogni grande rivoluzione tecnologica ha imposto una ridefinizione del quadro normativo. La rivoluzione digitale ha introdotto nuove tipologie di rischio — cybercrime, manipolazione dei dati, sorveglianza di massa — che le regolazioni preesistenti non erano attrezzate ad affrontare. Il diritto ha risposto con un'evoluzione continua che riflette la capacità di adattarsi alle trasformazioni imposte dall'innovazione: dal GDPR al Data Governance Act, dal Digital Services Act al Digital Markets Act, fino al Cybersecurity Act e alle direttive NIS.

In questo contesto si colloca il Regolamento UE 2024/1689, noto come AI Act, che rappresenta il primo tentativo di regolamentazione globale dell'intelligenza artificiale. L'Unione Europea si conferma come legislatore pioniere in materia digitale, esercitando quello che la dottrina chiama il «Brussels Effect»: la capacità di proiettare la propria regolamentazione oltre i confini territoriali, imponendo de facto standard globali che imprese e Stati terzi devono adottare per accedere al mercato unico europeo. Se questo effetto si produrrà anche per l'AI Act, e in quale misura, è oggetto di un dibattito ancora aperto.

7.2 L'architettura dell'AI Act: rischio come criterio ordinatore

Il principio fondamentale dell'AI Act è la proporzionalità: l'intensità dell'intervento regolatorio è calibrata in funzione del livello di rischio connesso all'impiego dell'IA. Il regolamento individua quattro categorie:

- Pratiche vietate: sistemi incompatibili con i diritti fondamentali, come il social scoring generalizzato, la manipolazione subliminale, il riconoscimento facciale in tempo reale negli spazi pubblici (con eccezioni limitate).
- Sistemi ad alto rischio: applicazioni con incidenza su settori strategici — sanità, istruzione, reclutamento, amministrazione della giustizia, infrastrutture critiche, controllo delle frontiere. Questi sistemi sono soggetti agli obblighi più stringenti.
- Tecnologie a rischio limitato: sistemi con obblighi specifici di trasparenza, come i chatbot (che devono dichiarare la propria natura artificiale) e i sistemi di riconoscimento delle emozioni.
- Sistemi a basso rischio: applicazioni esentate da vincoli stringenti — filtri antispam, videogiochi con IA, sistemi di raccomandazione — pur rientrando in un quadro di principi generali di affidabilità.

Il regolamento si applica all'intera catena di fornitura e utilizzo dell'IA: fornitori, distributori, deployer (utilizzatori), rappresentanti autorizzati e importatori. Per le imprese italiane, la categoria più rilevante è quella dei deployer — le organizzazioni che integrano sistemi di IA nei propri processi. Per un approfondimento si legga il quarto capitolo di questo documento.

7.3 Gli obblighi per le imprese che adottano sistemi ad alto rischio

Il legislatore europeo ha affidato al datore di lavoro, in quanto deployer, la valutazione dei rischi connessi all'utilizzo dell'IA e la responsabilità conseguente ai danni che essa può provocare. Si tratta di un impegno significativo, che presuppone investimenti in tecnologia, organizzazione e formazione, e che interseca normative già esistenti in materia di privacy, sicurezza sul lavoro e diritti dei lavoratori.

Gli obblighi dei deployer si articolano in quattro ambiti: sorveglianza (monitoraggio continuo del sistema per garantire il controllo umano e la capacità di intervento tempestivo), trasparenza (informare i lavoratori e i loro rappresentanti prima dell'impiego di sistemi ad alto rischio), integrità (verificare la qualità dei dati di input e conservare i log generati per almeno sei mesi), sicurezza (adottare misure tecniche e organizzative per garantire un utilizzo conforme alle istruzioni del fornitore).

Il primo obbligo già in vigore, dall'agosto 2024, riguarda l'alfabetizzazione digitale: i deployer devono garantire un livello adeguato di formazione e consapevolezza nell'utilizzo dei sistemi di IA. Prima della messa in servizio di sistemi ad alto rischio, è inoltre richiesta una valutazione di impatto sui diritti fondamentali.

L'AI Act impone una governance basata sull'analisi del rischio specifico al caso di specie: non esistono soluzioni uniformi valide per tutti. Ogni impresa deve costruire il proprio percorso di compliance, tenendo conto delle caratteristiche dei sistemi adottati, dei dati trattati e del contesto operativo. Questo è particolarmente impegnativo per le PMI, che spesso non dispongono delle strutture interne necessarie.

7.4 La responsabilità civile: un quadro ancora in evoluzione

L'AI Act introduce un piano sanzionatorio proporzionato alla gravità delle violazioni, ma non disciplina in modo esaustivo la responsabilità civile per danni causati dai sistemi IA. Questa rimane regolata dalle normative nazionali esistenti — in Italia, dal Codice Civile — con riferimento principale agli articoli sulla responsabilità per attività pericolose (art. 2050 c.c.) e sulla responsabilità del custode (art. 2051 c.c.).

La dottrina prevalente qualifica la responsabilità da IA come responsabilità oggettiva: per ottenere il risarcimento è sufficiente dimostrare il danno e il nesso causale con il funzionamento del sistema, senza necessità di provare la colpa dell'operatore. L'evoluzione giurisprudenziale è ancora in una fase embrionale, con interpretazioni prevalentemente concentrate sul diritto del lavoro — impiego privato e pubblico — dove i giudici hanno applicato principi consolidati come il divieto di discriminazione e la responsabilità organizzativa del committente.

Il riconoscimento della parità tecnologica tra imprese — il principio per cui tutte le organizzazioni, indipendentemente dalla dimensione, devono avere pari accesso alle nuove tecnologie — è un obiettivo importante ma la sua applicazione pratica deve tenere conto delle specificità delle PMI. L'iper-regolamentazione rischia di essere un ostacolo maggiore per le piccole imprese che per le grandi: un paradosso che il legislatore europeo dovrebbe considerare attentamente per evitare che la regolazione trasformi un'opportunità in un privilegio riservato a chi ha le risorse per navigarne la complessità.

8. Prospettive e priorità per l'Italia

Il report di Confindustria restituisce un'immagine dell'Italia sospesa tra opportunità riconosciuta e trasformazione incompiuta. I 241 casi d'uso documentati dimostrano che l'intelligenza artificiale non è un fenomeno del futuro: è già presente, già operativa, già in grado di produrre benefici concreti nelle imprese italiane più avanzate. Ma il divario tra questi pionieri e la grande massa del sistema produttivo — soprattutto le PMI — rimane ampio e preoccupante.

I dati ISTAT fotografano un Paese che, nel 2024, ha visto l'8,2% delle proprie imprese adottare almeno una tecnologia IA, contro il 13,5% della media europea. Un divario che non è puramente tecnico o finanziario: è anche culturale, organizzativo, formativo. Le barriere principali — costi elevati e mancanza di competenze — sono due facce della stessa moneta: senza competenze adeguate, gli investimenti in IA tendono ad essere meno efficaci, generando delusioni che a loro volta disincentivano ulteriori investimenti.

Le priorità che emergono dall'analisi sono chiare. Sul versante delle politiche pubbliche, servono interventi orizzontali di contesto — incentivi all'adozione, sostegno alla formazione, investimenti

in infrastrutture digitali — accompagnati da un approccio normativo che riduca la complessità burocratica per le PMI senza abbassare le garanzie di sicurezza e rispetto dei diritti. Sul versante del sistema Confindustria, la sfida è costruire una strategia di diffusione dell'IA che raggiunga capillarmente le piccole e medie imprese, attraverso strumenti di knowledge sharing, reti di competenza e supporto all'implementazione.

Il potenziale c'è: l'Italia ha un sistema produttivo manifatturiero di eccellenza, un patrimonio di know-how settoriale unico, e — come dimostrano i casi d'uso analizzati — imprenditori capaci di innovare quando vengono messi nelle condizioni di farlo. La questione non è se l'intelligenza artificiale trasformerà il sistema Italia, ma se questa trasformazione sarà guidata o subita, distribuita o concentrata, inclusiva o elitaria.

Non sarà un'IA a determinare il futuro dell'economia italiana. Saranno le scelte — di politica industriale, di investimento, di formazione, di governance — che le persone faranno nei prossimi anni. L'IA è uno strumento straordinariamente potente. Come ogni strumento, il suo impatto dipende da chi lo usa, come lo usa e con quale visione.

Capitolo 3 – La mappa mondiale dell'AI: la dimensione geopolitica dell'intelligenza artificiale

1. L'intelligenza artificiale come posta in gioco geopolitica

Comprendere l'intelligenza artificiale richiede oggi strumenti analitici che vanno ben oltre la tecnologia. Il ciclo di investimenti straordinari che ha preso avvio dalla fine del 2022 — guidato dalle grandi piattaforme tecnologiche statunitensi e incentrato sull'ecosistema di NVIDIA — non può essere letto attraverso le sole categorie dell'economia di mercato. È un fenomeno che appartiene a pieno titolo alla sfera della politica internazionale, alle dinamiche della competizione tra potenze, alle logiche della sicurezza nazionale. L'intelligenza artificiale è diventata una posta in gioco geopolitica di prima grandezza.

Tre chiavi interpretative permettono di orientarsi in questa complessità. La prima è il concetto di capitalismo politico: la crescente fusione tra logiche economiche e vincoli politici, che plasma le decisioni delle imprese e degli stati in modo inscindibile. La seconda è la continuità tra intelligenza artificiale e il più lungo processo di digitalizzazione e computerizzazione del mondo — una continuità che rende evidente il ruolo strutturale dell'ecosistema dei semiconduttori, non solo come industria ma come teatro di una competizione strategica globale. La terza è la dimensione fisica della tecnologia: i data center, i consumi energetici, le filiere di assemblaggio e le infrastrutture materiali senza le quali i sistemi di intelligenza artificiale semplicemente non esistono.

L'intelligenza artificiale è un software solo in una certa misura. Per il suo funzionamento è fondamentale una complessa struttura materiale: semiconduttori, data center, energia, acqua, acciaio, rame. Chi controlla questa infrastruttura esercita un potere che nessun algoritmo, per quanto sofisticato, può aggirare.

Questi tre ambiti — capitalismo politico, ecosistema dei semiconduttori, vincoli infrastrutturali — non sono separati: si intrecciano e si rinforzano reciprocamente, producendo una configurazione del potere globale che ridefinisce i rapporti di forza tra stati, tra imprese e tra sistemi economici. Comprendere l'intelligenza artificiale significa comprendere questo intreccio.

2. Il capitalismo politico: quando la sicurezza nazionale governa l'economia

2.1 Genealogia di un concetto

La nozione di capitalismo politico ha radici che affondano nel pensiero di Max Weber. Per Weber, la razionalizzazione che caratterizza il capitalismo moderno rappresenta storicamente una riduzione dei vincoli politici allo sviluppo economico: un processo in cui la gerarchia degli interessi si orienta verso il rischio d'impresa e il perseguimento del profitto. Tuttavia, Weber stesso — insieme a Werner Sombart — riconosceva che già all'alba del Novecento lo sviluppo delle burocrazie statali e la grande dimensione delle imprese avevano avviato una trasformazione della forma capitalistica classica, verso un sistema in cui il mercato convive con vincoli burocratici crescenti.

Aggiornato al contesto attuale, il capitalismo politico descrive un sistema in cui economia e politica si fondono in un'entità integrata: le decisioni economiche vengono plasmate direttamente e indirettamente da interessi di sicurezza nazionale e obiettivi politici. Questa fusione avviene sia nei sistemi democratici, come quello statunitense, sia nei sistemi autoritari, come quello cinese — con modalità diverse ma con un effetto convergente: l'allargamento dell'ambito di intervento del potere pubblico sull'economia attraverso la leva della sicurezza nazionale.

2.2 Le cinque caratteristiche del capitalismo politico contemporaneo

La prima caratteristica è la compenetrazione sistematica di economia e politica. Nei sistemi autoritari, questa compenetrazione coincide con la presenza capillare di un partito-stato nel governo centrale e locale, oltre che nelle imprese. Nei sistemi democratici, si esprime attraverso l'intrusività delle burocrazie della difesa e della sicurezza sulle libertà economiche, e attraverso poteri di emergenza che rendono possibile l'intervento statale.

La seconda caratteristica è l'uso politico del commercio e della finanza, con il progressivo abbandono di una visione dei rapporti economici fondata sull'interdipendenza mutualmente vantaggiosa e l'ascesa di una logica da gioco a somma zero. L'interdipendenza economica non scompare — da essa dipende la concreta possibilità di realizzare smartphone, automobili, data

center — ma viene affiancata da una logica di competizione e conflitto in cui le capacità industriali e i primati tecnologici vengono considerati come armi.

La terza caratteristica è la politicizzazione della tecnologia: il suo sviluppo, il suo possesso e il suo utilizzo vengono valutati in termini crescenti come fattori competitivi tra stati. Le imprese non operano in un contesto neutrale ma all'interno di schieramenti definiti politicamente. Questo ha effetti diretti sulle modalità con cui possono commerciare e realizzare i loro prodotti, esponendole a rischi politici crescenti.

La quarta caratteristica è la designazione di industrie strategiche — considerate essenziali per il perseguimento degli interessi nazionali — e di aziende «avversarie» — identificate come minacce per via della loro collocazione geografica. Queste industrie e aziende vengono protette o avversate non solo attraverso le partecipazioni al capitale (uno strumento tradizionale ma limitato), ma attraverso un arsenale di strumenti più sottili: vincoli all'accesso ai mercati, controlli sugli investimenti, liste nere, restrizioni sulle esportazioni.

La quinta caratteristica è l'armamentario giuridico con cui tutto questo si concretizza: sanzioni, meccanismi di monitoraggio delle filiere, uso politico dell'antitrust e delle norme sulla concorrenza, controlli sugli investimenti diretti esteri, limitazioni sulla possibilità di commerciare liberamente. Il diritto diventa uno strumento di geopolitica economica.

2.3 Le due potenze del capitalismo politico

Gli Stati Uniti dispongono di una vasta burocrazia della difesa e della sicurezza nazionale la cui pervasività è difficile da comprendere senza guardare ai numeri: una spesa per la difesa di circa 850 miliardi di dollari per l'anno fiscale 2025, di cui oltre 140 miliardi destinati a ricerca, sviluppo, test e valutazioni. Circa 750 basi militari all'estero. Oltre cinque milioni di individui con accesso a documenti classificati. Il concetto di «base industriale della difesa» — il complesso di imprese che partecipano alle forniture delle forze armate — illustra quanto profondamente il vincolo della sicurezza nazionale sia intrecciato con il tessuto economico privato.

La Cina del presidente Xi Jinping ha percorso negli ultimi quarantacinque anni una traiettoria di ascesa economica senza precedenti, costruendo un sistema di strette relazioni tra potere politico e

potere economico. Il Partito Comunista Cinese, con quasi cento milioni di membri nel 2024, controlla il territorio cinese nel governo centrale e locale, e si estende alle imprese attraverso cellule interne. Il controllo varia da settore a settore — più pervasivo nel finanziario, meno nel manifatturiero — e coesiste con un'innovazione che avviene principalmente nell'ambito privato. Ma il confine tra privato e politico rimane poroso: la vicenda dell'imprenditore Jack Ma, co-fondatore di Alibaba, la cui critica pubblica alla regolamentazione finanziaria nel 2020 determinò il blocco della quotazione di Ant e la sua sostanziale sparizione dalla scena pubblica per mesi, illustra con chiarezza i vincoli che la libertà economica incontra quando sfida la distribuzione del potere politico.

Made in China 2025, l'iniziativa strategica lanciata nel 2015 con l'obiettivo di trasformare la Cina da produttore di beni a basso costo a leader mondiale in settori ad alta tecnologia, ha definito per un decennio la percezione internazionale della strategia economica cinese. Nonostante Pechino abbia progressivamente ridotto la presenza di questo piano nel discorso pubblico — in risposta alle preoccupazioni sollevate dai partner commerciali — gli obiettivi strategici rimangono pienamente integrati nelle politiche industriali cinesi, soprattutto nei settori fondamentali.

3. L'ecosistema dei semiconduttori: filiere, nicchie e guerra invisibile

3.1 Una storia di primati e vulnerabilità

Dalla fine della Seconda guerra mondiale, la storia della microelettronica coincide con la storia del primato tecnologico americano. Le innovazioni dei laboratori Bell di AT&T — a partire dalla scoperta del transistor nel 1947 — e le commesse del Pentagono negli anni Cinquanta e Sessanta hanno dato vita alla Silicon Valley e a imprese fondamentali come Fairchild Semiconductor e Intel. Il nome stesso di questa valle californiana richiama l'industria che l'ha generata.

La competizione con il Giappone, negli anni Settanta e Ottanta, offrì il primo segnale di quanto fosse vulnerabile questo primato. Le aziende giapponesi — NEC, Toshiba, Hitachi — conquistarono rapidamente quote di mercato nella produzione di chip di memoria DRAM, sfruttando tecniche organizzative e produttive superiori e pratiche commerciali aggressive, incluso il dumping. Tra il

1978 e il 1986, la quota statunitense nel mercato dei DRAM scese dal 70% al 20%, mentre quella giapponese salì dal 30% al 75%.

La risposta degli Stati Uniti fu istruttiva per il futuro: non solo accordi commerciali, ma una crescente politicizzazione del settore. La minacciata acquisizione di Fairchild Semiconductor da parte di Fujitsu nel 1986 scatenò una reazione che avrebbe avuto effetti duraturi: il Congresso approvò nel 1988 l'emendamento Exon-Florio, istituendo il potere presidenziale di bloccare fusioni e acquisizioni straniere che mettono in pericolo la sicurezza nazionale, previa istruttoria del CFIUS — Committee on Foreign Investments in the United States. Gli Stati Uniti emergeranno vincitori dalla guerra dei semiconduttori con il Giappone negli anni Novanta, grazie alla stagnazione economica giapponese, alla collaborazione più stretta tra governo e imprese, e alla capacità di Intel di cogliere l'innovazione decisiva del decennio: la diffusione capillare dei personal computer.

3.2 La struttura che ha cambiato tutto: il modello fabless

Negli stessi anni Ottanta e Novanta in cui si svolgeva la guerra con il Giappone, l'industria dei semiconduttori viveva la sua trasformazione strutturale più profonda, i cui effetti durano fino ad oggi. Si tratta della separazione tra progettazione e produzione. Morris Chang, ingegnere e imprenditore nato nel 1931 in Cina, dopo una lunga carriera in Texas Instruments si trasferisce a Taiwan nella seconda metà degli anni Ottanta su invito della classe dirigente dell'isola. Nel 1987 fonda TSMC — Taiwan Semiconductor Manufacturing Company — sulla base di una tesi semplice ma rivoluzionaria: i costi crescenti delle fabbriche per semiconduttori avanzati rendono insostenibile per molte aziende mantenere insieme progettazione e produzione. La soluzione è la specializzazione totale: alcune aziende si concentreranno esclusivamente sulla produzione (le foundry), altre esclusivamente sul design.

Questa separazione ha generato l'ecosistema attuale. Sul versante del design, un fiorente universo di aziende fabless — NVIDIA, AMD, Broadcom, Qualcomm, Apple — che progettano chip senza possedere fabbriche. Sul versante della produzione, un oligopolio ristrettissimo dominato da TSMC, affiancata dalla coreana Samsung e, con crescenti difficoltà, da Intel. E intorno a questi due poli, centinaia di aziende specializzate in nicchie indispensabili: il software di progettazione (Synopsys e Cadence Systems, entrambe americane), la chimica e i materiali, gli strumenti e i macchinari

(dove ASML dei Paesi Bassi detiene un monopolio de facto nelle macchine per la litografia a ultravioletti estremi), l'assemblaggio e i test (concentrati a Taiwan, in Corea del Sud e nel Sud-Est asiatico).

Questa diversificazione crea quello che in gergo si chiama «collo di bottiglia»: nicchie di specializzazione così concentrate in una o poche aziende che la loro interruzione potrebbe fermare l'intera filiera — e con essa la digitalizzazione del mondo. Un giro d'affari globale superiore ai 600 miliardi di dollari, con previsioni che superano i 1.000 miliardi entro il 2030, dipende da questi equilibri fragili.

3.3 La seconda guerra dei semiconduttori: Stati Uniti contro Cina

L'ascesa della Repubblica Popolare Cinese come potenza tecnologica ha aperto una seconda guerra dei semiconduttori, per molti aspetti più complessa della prima. In pochi decenni, la Cina è passata da quote di mercato trascurabili a un peso significativo nell'elettronica, nelle telecomunicazioni e nell'automotive. Nella logica di Made in China 2025, Pechino ha investito crescentemente nei semiconduttori — sostenendo produttori come SMIC — e ha utilizzato la propria ascesa nell'elettronica di consumo per sviluppare capacità di progettazione. La divisione di design di Huawei, all'epoca tra i maggiori produttori mondiali di smartphone, nel 2019 era diventata il secondo cliente globale di TSMC dopo Apple.

Il 2018 ha segnato la svolta. L'arresto in Canada della direttrice finanziaria di Huawei, Meng Wanzhou — figlia del fondatore dell'azienda — su mandato statunitense per presunte violazioni delle sanzioni verso Iran e Corea del Nord, ha inaugurato una fase di escalation che non si è mai interrotta. Gli Stati Uniti hanno progressivamente rafforzato i controlli sulle esportazioni verso Huawei, imponendo alle aziende della filiera americana — inclusi i produttori di macchinari — di operare attraverso licenza governativa per qualsiasi transazione con la società cinese. Senza il contributo americano, TSMC stessa non può produrre per Huawei.

Il 7 ottobre 2022, il Bureau of Industry and Security del Dipartimento del Commercio ha pubblicato un ampio pacchetto di misure che ha radicalmente ampliato questa logica: restrizioni sull'accesso cinese al supercalcolo e all'intelligenza artificiale, limitazioni alla cooperazione di cittadini

statunitensi con imprese cinesi, obblighi di trasparenza sulle clientele finali delle aziende cinesi, interventi su tutta la supply chain — non solo i chip finiti, ma anche software, progettazione e macchinari. Parallelamente, il CHIPS & Science Act del 2022 ha stanziato decine di miliardi di dollari per attrarre investimenti produttivi di TSMC, Intel e Samsung sul suolo americano, puntando a ridurre la concentrazione geografica di una filiera percepita come strategicamente vulnerabile.

La Cina risponde con investimenti massicci nell'autosufficienza. Huawei — duramente colpita nei ricavi dalle misure americane — diventa il capofiliera dei semiconduttori nell'ecosistema domestico cinese. BYD, campione della mobilità elettrica, acquisisce fabbriche di chip. SMIC e CXMT ampliano le proprie capacità produttive: la Cina è oggi il secondo acquirente mondiale di attrezzature per fabbriche di semiconduttori, subito dopo TSMC, davanti a qualsiasi azienda americana. «Nei semiconduttori, non c'è più globalizzazione; non c'è più libero commercio. La priorità è solo la sicurezza nazionale.» — Morris Chang, fondatore di TSMC, 2023.

Malgrado questi sforzi, la Cina rimane vulnerabile in segmenti cruciali: i macchinari di litografia avanzata (dove ASML ha un monopolio che le esportazioni verso la Cina sono state progressivamente bloccate da olandesi e americani), il software di progettazione, le GPU ad alte prestazioni. Made in China 2025 ha prodotto risultati, ma non l'autosufficienza sperata — sia per la complessità intrinseca della filiera, sia per la sofisticazione crescente delle misure di contenimento occidentali.

4. La materialità dell'intelligenza artificiale: data center, energia e filiere

4.1 Memphis, Tennessee: il nuovo volto dell'infrastruttura IA

Due luoghi geografici permettono di afferrare concretamente la dimensione fisica dell'intelligenza artificiale, al di là delle astrazioni dei modelli linguistici e degli algoritmi. Il primo è Memphis, Tennessee, dove Elon Musk — attraverso la sua startup xAI — ha realizzato nel 2024 il supercomputer Colossus: un cluster di 100.000 GPU NVIDIA H100 che si posiziona tra i centri di addestramento IA più potenti al mondo. La velocità di realizzazione — 19 giorni, secondo le

dichiarazioni del CEO di NVIDIA Jensen Huang — è di per sé un indicatore dell'intensità della competizione infrastrutturale in atto.

Le dimensioni dell'impatto di Colossus sull'ambiente circostante sono eloquenti. Il supercomputer richiede fino a 150 megawatt di potenza all'ora durante i picchi di carico — l'equivalente del consumo elettrico quotidiano di circa 120.000 famiglie americane. I sistemi di raffreddamento richiedono circa 1,3 milioni di galloni d'acqua al giorno. Queste necessità hanno generato preoccupazioni ambientali e infrastrutturali significative nella comunità locale di Memphis, aprendo un fronte di tensione tra le esigenze della corsa all'IA e i diritti delle comunità che ospitano queste infrastrutture.

L'episodio di Colossus non è isolato: è il punto più visibile di una tendenza che nel 2024 ha portato le maggiori aziende tecnologiche americane — Google, Amazon, Microsoft — a riconsiderare persino l'energia nucleare come fonte stabile per i propri data center. Microsoft ha siglato un accordo con Constellation Energy per riavviare un'unità della centrale nucleare di Three Mile Island in Pennsylvania — teatro del più grave incidente nucleare nella storia degli Stati Uniti, nel 1979 — con un investimento stimato di 1,6 miliardi di dollari e un impegno ad acquistarne l'intera produzione energetica. Amazon Web Services ha acquisito per 650 milioni di dollari un campus di data center in Pennsylvania alimentato direttamente da una centrale nucleare. L'IA sta letteralmente riaccendendo reattori nucleari spenti.

4.2 Guadalajara, Messico: la filiera che non si vede

Il secondo luogo emblematico è Guadalajara, in Messico, dove il principale assemblatore di elettronica al mondo, Foxconn, ha annunciato nell'ottobre 2024 la costruzione di una gigantesca fabbrica per la produzione di server per l'intelligenza artificiale. Il significato di questo annuncio è duplice. Sul piano produttivo, documenta il processo con cui i componenti dei sistemi NVIDIA — realizzati in molteplici unità produttive sparse per il mondo — vengono assemblati in server che poi raggiungono i clienti finali: Microsoft, Google, Meta, Apple, Oracle, Tesla e altri. Sul piano geopolitico, segnala una ridefinizione della geografia produttiva globale.

La scelta del Messico non è casuale. Due fattori la spiegano: la prossimità agli Stati Uniti, che consente di rafforzare una filiera nordamericana integrata in ottica anticinese; e la forza lavoro, a

basso costo e già organizzata per le produzioni manifatturiere complesse. È una delle ironie più acute del momento storico: i lavoratori messicani, oggetto di ostilità politica quando si trovano sul suolo americano, diventano indispensabili — e invisibili agli occhi degli elettori americani — per assemblare i server su cui si costruisce il primato tecnologico degli Stati Uniti.

L'annuncio di Foxconn si inscrive in una più ampia ridefinizione della geografia produttiva globale. Il modello centrato sulla Cina come fabbrica del mondo si sta frammentando, con la diversificazione verso Vietnam, Malaysia, Messico e India. Il Paese più popoloso del mondo è in teoria capace di fornire le stesse economie di scala della Cina, ma le sue filiere produttive sono ancora meno mature. Il Sud-Est asiatico offre una buona base manifatturiera in alcuni ecosistemi e capacità organizzative consolidate. La riconfigurazione è in corso, ma è un processo lento e costoso: le competenze industriali che si sono stratificate in Cina nel corso di decenni non si replicano rapidamente.

4.3 NVIDIA al centro dell'ecosistema

La comprensione della dimensione fisica dell'intelligenza artificiale passa necessariamente attraverso NVIDIA. Fondata nel 1993 da Jensen Huang — ingegnere elettronico nato a Taiwan e trasferitosi negli Stati Uniti prima dei dieci anni — l'azienda si è evoluta da produttrice di schede grafiche per videogiochi a protagonista assoluta dell'era dell'IA. Il momento decisivo di questa trasformazione è individuabile nel 2012: i ricercatori Geoffrey Hinton, Alex Krizhevsky e Ilya Sutskever dell'Università di Toronto utilizzano le schede grafiche NVIDIA per sviluppare AlexNet, un modello di rete neurale che rivoluziona il riconoscimento delle immagini e inaugura l'era del deep learning contemporaneo.

NVIDIA aveva investito per anni nello sviluppo di schede grafiche per il calcolo scientifico, anticipando un mercato che non era ancora evidente. Questo investimento di lungo termine le ha permesso di cogliere quello che Jensen Huang stesso ha definito «il momento iPhone dell'intelligenza artificiale» — il lancio di ChatGPT alla fine del 2022. Il segmento dei data center di NVIDIA, che generava ricavi per circa 200 milioni di dollari nel 2014, ha superato i 100 miliardi di dollari nel 2023: una crescita di cinquecento volte in meno di un decennio.

La catena di dipendenza è nitida: senza l'ecosistema dei semiconduttori non esistono i prodotti NVIDIA; senza i prodotti NVIDIA non esistono i data center dove avviene l'addestramento dei modelli di IA; senza i data center non esiste ChatGPT. E senza ChatGPT — o i suoi equivalenti — non esiste il ciclo di investimenti che attualmente muove centinaia di miliardi di dollari. Ogni anello di questa catena è fisicamente situato da qualche parte nel mondo, con specifici requisiti di energia, acqua, materiali e manodopera specializzata.

5. Dipendenze strutturali e potere di mercato

Le aziende che si presentano come protagoniste dell'intelligenza artificiale — OpenAI, DeepMind, Anthropic — non sono mai realmente autonome. OpenAI dipende da Microsoft per le infrastrutture di calcolo essenziali al funzionamento e all'addestramento dei propri modelli. DeepMind è di proprietà di Google dal 2014. Anthropic — fondata da ex ricercatori di OpenAI — è sostenuta da Amazon e Google. Queste dipendenze non sono contingenti: sono strutturali, perché i costi delle infrastrutture di calcolo necessarie per sviluppare modelli di frontiera sono nell'ordine di miliardi di dollari, inaccessibili per qualsiasi entità che non abbia accesso a capitali di scala analoga.

I continui investimenti necessari per sostenere questi costi rendono difficile — se non impossibile — che le startup dell'IA si possano svincolare dai loro principali finanziatori. Per farlo, dovrebbero generare autonomamente ricavi e profitti in grado di coprire i costi infrastrutturali. La finestra temporale in cui un'azienda come OpenAI potrebbe teoricamente raggiungere questa autonomia è incerta, e si restringe man mano che i costi di addestramento dei modelli crescono.

Alcune di queste aziende — OpenAI in primo luogo — hanno manifestato la volontà di ridurre la dipendenza controllando più direttamente la propria filiera infrastrutturale: progettando i semiconduttori di cui hanno bisogno (sempre con il contributo di aziende competenti come Broadcom) o addirittura producendo elettronica. Tuttavia, come osserva Aresu, queste ambizioni si scontrano con un limite strutturale: le competenze industriali e tecnologiche che caratterizzano l'ecosistema dei semiconduttori si sono stratificate nel tempo attraverso decenni di investimento, di apprendimento e di fallimento. Non possono essere replicate in pochi anni, indipendentemente dalla disponibilità di capitali.

In sostanza le startup dell'IA dipendono dai grandi hyperscaler per le infrastrutture di calcolo. Gli hyperscaler dipendono da NVIDIA per le GPU. NVIDIA dipende da TSMC per la produzione. TSMC dipende da ASML per i macchinari di litografia. E ASML dipende da una catena di centinaia di fornitori specializzati. Ogni nodo di questa catena è un potenziale vettore di pressione politica.

Questa catena di dipendenze è anche una mappa del potere reale nell'ecosistema dell'intelligenza artificiale. Chi controlla i nodi strategici — i colli di bottiglia — esercita un'influenza che va ben oltre la propria quota di mercato. È per questo che i controlli sulle esportazioni americani di macchinari e chip verso la Cina sono così efficaci: colpendo poche aziende in posizione dominante (ASML per i macchinari di litografia, NVIDIA per le GPU di training), riescono a limitare l'accesso cinese all'intero ecosistema.

6. Punti di forza e vulnerabilità delle due potenze

6.1 Il vantaggio americano e i suoi limiti

Gli Stati Uniti mantengono una posizione dominante nella potenza di calcolo per l'intelligenza artificiale. I cluster di addestramento più avanzati del mondo sono localizzati in territorio americano e si basano su centinaia di migliaia di GPU NVIDIA — le uniche disponibili alle prestazioni richieste dai modelli di frontiera. Questo vantaggio è cruciale per lo sviluppo di sistemi di IA avanzata e per il mantenimento del primato tecnologico nella competizione con la Cina.

Tuttavia, questo vantaggio non è privo di limiti. Il principale è energetico: le infrastrutture elettriche americane faticano a tenere il passo con le esigenze di calcolo dell'intelligenza artificiale. Normative complesse, vincoli regolatori e mancanza di strutture dedicate limitano la crescita su larga scala dei data center. La risposta — il ritorno all'energia nucleare, gli accordi con centrali dismesse, la distribuzione delle operazioni di calcolo tra data center geograficamente dispersi — è costosa e lenta. La Federal Energy Regulatory Commission ha già bloccato alcuni accordi di interconnessione, segnalando che le resistenze regolamentari non sono trascurabili.

6.2 I vantaggi cinesi e le vulnerabilità persistenti

La Cina presenta un profilo competitivo complementare e per certi versi speculare. Il vantaggio cinese non è nella qualità dei chip — dove il divario tecnologico con il fronte occidentale rimane significativo — ma nella flessibilità infrastrutturale. La capacità di riconvertire rapidamente siti industriali esistenti in data center — impianti di produzione di alluminio trasformati in centri di calcolo in meno di sei mesi, secondo stime di ricercatori specializzati — consente alla Cina di costruire capacità computazionale con una velocità che le strutture normative e burocratiche americane non permettono.

Huawei è l'attore centrale di questa espansione. Pur avendo subito perdite pesanti di ricavi e profitti per effetto delle misure americane, è diventata il capofiliera dei semiconduttori nell'ecosistema domestico cinese, con investimenti stimati in 7,3 miliardi di dollari solo nel 2024 per lo sviluppo di fabbriche avanzate. Grazie anche alla collaborazione con SMIC e CXMT, la Cina è diventata il secondo acquirente mondiale di attrezzature per la produzione di semiconduttori.

Le vulnerabilità cinesi rimangono tuttavia strutturali. I chip cinesi più avanzati non raggiungono le prestazioni delle GPU NVIDIA nelle applicazioni di training dei grandi modelli linguistici. I macchinari di litografia avanzata — il collo di bottiglia più critico — non sono producibili internamente a livelli competitivi, e l'accesso a quelli occidentali è progressivamente bloccato. Made in China 2025, pur avendo portato alcuni risultati, non ha generato la tanto agognata autosufficienza, e i tempi per colmare il divario tecnologico si allungano man mano che le misure di contenimento americane si fanno più sofisticate.

7. Le terre rare: il sottosuolo che governa l'intelligenza artificiale

Dietro ogni modello linguistico di frontiera, ogni acceleratore grafico, ogni data center che alimenta la corsa globale all'intelligenza artificiale, vi è una catena di approvvigionamento che affonda le proprie radici — letteralmente — nel sottosuolo di pochi paesi. Le terre rare, un gruppo di diciassette elementi metallici che comprende i quindici lantanidi più scandio e ittrio, costituiscono la materia prima indispensabile per la fabbricazione di magneti permanenti ad alte prestazioni, semiconduttori avanzati, memorie ad alta densità e componenti optoelettronici. Senza

neodimio, praseodimio e disprosio non esistono i magneti che equipaggiano i sistemi di raffreddamento dei server; senza gallio e germanio non si producono i chip di potenza e i sistemi a infrarossi integrati nelle infrastrutture di difesa e telecomunicazione. La denominazione "rare" è, dal punto di vista geologico, in parte impropria: questi elementi non sono scarsi in senso assoluto, ma la loro concentrazione in giacimenti economicamente sfruttabili è geograficamente assai ristretta, e la loro raffinazione richiede processi chimici costosi, energivori e con pesanti impatti ambientali.

La produzione mondiale di terre rare ha raggiunto nel 2024 le 390.000 tonnellate, più che triplicando il volume estratto nel 2017, a testimonianza della pressione crescente esercitata dalla transizione digitale e dall'accelerazione dell'IA. Ma la crescita della produzione non ha distribuito geograficamente il potere: al contrario, lo ha ulteriormente concentrato. La Cina estrae circa 270.000 tonnellate all'anno e detiene riserve stimate in 44 milioni di tonnellate, pari a circa un terzo delle riserve mondiali totali — stimate complessivamente in 130 milioni di tonnellate. Più rilevante ancora del dato estrattivo è il controllo che Pechino esercita sulla fase di raffinazione e trasformazione: secondo le stime più recenti, la Cina controlla oltre il 90% della capacità mondiale di raffinazione delle terre rare e quasi la totalità della produzione industriale di magneti permanenti di precisione, che sono i componenti critici per motori elettrici, turbine eoliche e — con crescente rilevanza — per i sistemi di raffreddamento e attuazione meccanica dei data center. Questa concentrazione non è il frutto di vantaggi geologici superiori, ma di decenni di investimenti pubblici deliberati, costi ambientali esternalizzati e politica industriale di lungo periodo.

Tabella 1 — Principali paesi per riserve e produzione di terre rare (dati U.S. Geological Survey, 2025)

Paese	Riserve stimate (Mt)	Produzione 2024 (t)	Note strategiche
Cina	44,0	270.000	Primo estrattore e raffinatore mondiale
Vietnam	22,0	300	Riserve ingenti, sfruttamento ancora limitato
Brasile	21,0	n.d.	Riserve quasi inesplorate
Australia	25,7	18.000	Principale alternativa extra-Cina
India	6,9	2.900	Produzione stagnante, potenziale elevato
Russia	3,8	n.d.	Integrazione in filiere proprie
Stati Uniti	1,9	45.000	Miniera Mountain Pass; dipendenza strutturale
Groenlandia	1,5	—	Giacimenti critici, oggetto di pressioni geopolitiche

Fonte: U.S. Geological Survey – Mineral Commodity Summaries 2025. Mt = milioni di tonnellate metriche. I dati di produzione si riferiscono alle stime 2024.

Oltre alla Cina, la mappa delle riserve rivela alcune concentrazioni geografiche di primo piano. Il Vietnam detiene riserve stimate intorno ai 22 milioni di tonnellate, seconde soltanto a quelle cinesi, ma lo sfruttamento rimane largamente sottosviluppato a causa di ostacoli istituzionali e infrastrutturali. Il Brasile possiede giacimenti stimati in 21 milioni di tonnellate pressoché inesplorati. L'Australia, con 25,7 milioni di tonnellate di riserve e una produzione di circa 18.000 tonnellate nel 2023, rappresenta il principale produttore alternativo, in particolare attraverso la società Lynas Rare Earths, l'unica al di fuori della Cina a gestire impianti di trasformazione su scala significativa — parte dei quali realizzati in Malesia. Gli Stati Uniti, con riserve limitate a 1,9 milioni di tonnellate, sono il secondo produttore mondiale grazie alla miniera di Mountain Pass in California, con circa 45.000 tonnellate estratte nel 2024, ma dipendono ancora massicciamente dall'importazione per le fasi di raffinazione e trasformazione. Di crescente interesse geopolitico è la Groenlandia, il cui sottosuolo ospita giacimenti significativi di terre rare pesanti — proprio quelle più critiche per le applicazioni ad alta tecnologia — e che è diventata oggetto esplicito di pressioni e attenzioni strategiche da parte degli Stati Uniti, dell'Unione europea e della stessa Cina.

Il nesso tra terre rare e intelligenza artificiale si è reso drammaticamente visibile nel biennio 2024-2025, quando la Cina ha progressivamente trasformato il controllo sulle proprie risorse minerarie in uno strumento di pressione geopolitica esplicita. In agosto 2023 Pechino ha introdotto licenze obbligatorie per l'esportazione di gallio e germanio, elementi critici per la produzione di semiconduttori avanzati, chip GaN e sistemi optoelettronici: le esportazioni verso Stati Uniti ed Europa sono crollate in poche settimane. Nel dicembre 2024, il governo cinese ha formalizzato il divieto di esportazione verso gli Stati Uniti di gallio, germanio, antimonio e grafite. Nell'aprile 2025, in risposta all'escalation dei dazi statunitensi, Pechino ha esteso le restrizioni a sette elementi chiave delle terre rare pesanti — tra cui disprosio, terbio, ittrio e scandio — e ai magneti permanenti da essi derivati, tagliando di fatto l'accesso ai produttori di armamenti, veicoli elettrici e componenti per l'IA. Il Parlamento europeo ha definito queste misure "ingiustificate" e coercitive, vista la posizione quasi monopolistica della Cina, e ha invitato la Commissione ad accelerare l'attuazione del Critical Raw Materials Act (CRMA). Un accordo sospensivo è stato raggiunto al vertice Trump-Xi del novembre 2025, ma la moratoria è limitata al 2026 e la struttura della dipendenza rimane intatta.

Per l'intelligenza artificiale le implicazioni economiche sono di prima grandezza. I chip GPU di nuova generazione necessari per addestrare modelli di frontiera — come quelli prodotti da NVIDIA, che controlla tra l'80 e il 90% del mercato degli acceleratori AI — richiedono materiali la cui filiera di approvvigionamento dipende ancora in misura strutturale dalla Cina. Secondo le stime dell'Agenzia Internazionale dell'Energia, il consumo energetico globale dei data center destinati all'IA crescerà dai 415 TWh del 2024 a circa 945 TWh nel 2030, equivalente all'intero fabbisogno elettrico del Giappone: un'espansione che richiederà un'accelerazione parallela nella costruzione di infrastrutture hardware che incorporano terre rare a ogni livello della catena tecnologica. Le dipendenze si sovrappongono e si moltiplicano: gli Stati Uniti dipendono dalla Cina per circa l'80% dei minerali critici, e da Taiwan per circa il 92% dei chip più avanzati. L'Europa si trova in una posizione ancor più esposta, non avendo né produzione mineraria propria di rilievo né grandi player nell'hardware IA.

Le risposte strategiche in corso sono molteplici ma ancora insufficienti a modificare gli equilibri nel breve periodo. Gli Stati Uniti hanno avviato il programma "Project Vault", una riserva strategica da 12 miliardi di dollari pensata come partenariato pubblico-privato per accumulare scorte di oltre

cinquanta elementi critici, e hanno stretto accordi con partner come la Corea del Sud per costruire capacità di raffinazione domestica di gallio e germanio. L'Unione europea ha adottato il Critical Raw Materials Act, che fissa obiettivi ambiziosi — estrarre almeno il 10% del proprio fabbisogno di minerali critici in Europa, processarne il 40% e diversificare le importazioni entro il 2030 — e ha avviato accordi di partenariato con paesi come Canada, Cile, Kazakhstan e alcuni stati africani. La Nigeria, che nel 2024 ha firmato un accordo di cooperazione con la Francia per lo sviluppo delle proprie riserve di terre rare, rappresenta un esempio della più ampia corsa diplomatica per ridisegnare le catene di fornitura. La Groenlandia è diventata uno dei fronti più caldi di questa competizione, con investimenti esplorativi promossi da attori europei, americani e cinesi.

Il punto critico che accomuna tutte queste strategie di diversificazione è che la sfida non riguarda solo l'estrazione, ma la raffinazione e la trasformazione in componenti industriali utilizzabili. Come hanno sottolineato diversi analisti al World Bank Mining Forum 2024, la vera competizione non si gioca nelle miniere, ma negli impianti di separazione, metallizzazione e produzione di magneti permanenti: ed è in questa fase, con l'85% della capacità globale di separazione concentrata in Cina, che il vantaggio competitivo di Pechino risulta più difficile da erodere. Costruire la capacità di raffinazione richiede anni, investimenti ingenti, tecnologie proprietarie e la disponibilità ad accettare i costi ambientali che in Europa e Nord America trovano maggiori resistenze politiche. Nel frattempo, il mercato globale delle terre rare è destinato a superare i 20 miliardi di dollari entro il 2031, con un tasso di crescita annuo superiore al 7%, spinto proprio dall'accelerazione dell'IA e dalla transizione energetica.

In sintesi, le terre rare rappresentano il piano materiale più profondo — e più spesso trascurato nel dibattito pubblico — della geopolitica dell'intelligenza artificiale. Chi controlla l'estrazione, la raffinazione e la commercializzazione di questi elementi detiene una leva di potere che si traduce in capacità di condizionare la produzione di chip, la costruzione di data center, l'autonomia delle industrie della difesa e, in ultima analisi, la velocità con cui ciascuna regione del mondo può sviluppare e dispiegare sistemi di IA avanzati. In questo senso, la competizione sulle terre rare non è una questione separata dalla regolazione dell'intelligenza artificiale o dalla geopolitica digitale: è il suo substrato fisico, la condizione materiale su cui poggiano tutte le architetture normative, le strategie di sovranità digitale e le ambizioni tecnologiche dei prossimi decenni.

8. Prospettive: la mappa del futuro prossimo

Alcuni scenari sembrano ragionevolmente prevedibili nel breve e medio termine. Il primo è la continuazione dell'escalation nelle restrizioni tecnologiche. Ogni ciclo di sanzioni americane genera una risposta cinese — nuovi investimenti nell'autosufficienza, nuovi capifiliera — che a sua volta giustifica un nuovo giro di restrizioni. Questa spirale non ha un punto di equilibrio naturale, ed è destinata ad accentuarsi man mano che entrambe le potenze accumulano capacità tecnologiche e aumentano le proprie vulnerabilità percepite.

Il secondo scenario è la ridefinizione della geografia produttiva globale. Il processo di diversificazione dalla centralità della Cina verso Vietnam, Malaysia, Messico e India è già in corso. Le monarchie del Golfo — con ingenti capitali disponibili — si trovano a dover scegliere con quale dei contendenti schierarsi per le proprie operazioni nei fondi e nelle società tecnologiche. L'India emerge come potenziale alternativa di scala alla Cina, ma le sue filiere produttive manifatturiere sono ancora in costruzione e richiedono tempo.

Il terzo scenario è la crescita del rilievo infrastrutturale nel discorso pubblico. La domanda energetica dei data center non è destinata a ridursi: ogni avanzamento nei modelli di IA richiede più calcolo, più energia, più acqua. Il ritorno all'energia nucleare, già iniziato, è destinato ad accelerare. Le comunità locali che ospitano queste infrastrutture diventeranno soggetti politici rilevanti, portando tensioni tra le esigenze della corsa tecnologica e i diritti locali all'interno del dibattito democratico.

Il quarto scenario è la crescente importanza dei capitali come fattore discriminante. L'addestramento dei modelli di IA richiede investimenti infrastrutturali nell'ordine di miliardi di dollari che solo pochi attori possono sostenere. Questo concentra ulteriormente il potere all'interno di un ecosistema già dominato da pochissime piattaforme. Le startup di IA — per quanto talentose e innovative — rimarranno strutturalmente dipendenti dagli hyperscaler che finanziano le loro infrastrutture.

L'intelligenza artificiale non è un settore tecnologico neutrale che si sviluppa secondo le sue logiche interne. È un terreno di competizione geopolitica dove si decidono i rapporti di forza del ventunesimo secolo. Comprenderla richiede leggere insieme algoritmi e geopolitica, codice e

acciaio, modelli linguistici e basi militari. La separazione tra queste dimensioni è una finzione intellettuale che la realtà si incarica sistematicamente di smentire.

La lezione finale del saggio di Aresu è che l'intelligenza artificiale non è un settore tecnologico che si sviluppa secondo la propria logica interna. È un terreno di competizione geopolitica dove le logiche del capitalismo politico plasmano ogni investimento, ogni acquisizione, ogni decisione di export control. Chi vorrà comprendere l'IA nei prossimi anni dovrà imparare a leggere insieme algoritmi e geopolitica, architetture neurali e filiere industriali, modelli linguistici e politiche di sicurezza nazionale. La separazione tra queste dimensioni è una finzione intellettuale che la realtà si incarica sistematicamente di smentire.

Capitolo 4 – Regolare l'Intelligenza Artificiale

1. Tre potenze, tre filosofie normative

1.1 Geopolitica della regolazione: perché le regole non sono mai neutre

Quando si osservano le tre aree geopolitiche che oggi guidano lo sviluppo dell'intelligenza artificiale — l'Unione europea, gli Stati Uniti e la Cina — emerge con chiarezza che le scelte normative non sono mai puramente tecniche, ma riflettono interessi economici e strategici profondamente diversi. Ciascuna di queste regioni ha costruito un proprio modello regolatorio coerente con la propria posizione nell'ecosistema tecnologico globale.

L'Europa si trova in una posizione peculiare: non dispone di investimenti paragonabili a quelli statunitensi o cinesi, né di imprese leader nel settore dell'IA. L'industria digitale di scala — da Google a Tencent — si è sviluppata altrove. Di fronte a questo gap strutturale, l'Unione europea ha scelto di competere non sul terreno della tecnologia, ma su quello delle regole, puntando ad affermare la propria capacità di normazione come leva di influenza globale.

Gli Stati Uniti, al contrario, ospitano i principali produttori di tecnologie di IA e adottano un approccio che lascia ampio spazio di autodeterminazione alle imprese. Il modello statunitense si fonda su meccanismi di autoregolazione e coregolazione, con il diritto della concorrenza come strumento di intervento pubblico residuale. Significativo è l'impegno volontario assunto nel giugno 2023 da sette grandi operatori del settore — tra cui Amazon, Anthropic, Google, Meta, Microsoft e OpenAI — ad assicurare uno sviluppo sicuro, affidabile e trasparente dell'IA secondo principi di safety, security e trust, seguito a breve distanza dall'Executive Order presidenziale sullo sviluppo sicuro e affidabile dell'intelligenza artificiale. Questo schema riflette le caratteristiche di un mercato in cui le grandi corporation, più che il legislatore, definiscono di fatto le regole del gioco, contrattuali e tecnologiche.

La Cina, dal canto suo, ha costruito negli anni un impianto normativo organico, che intreccia sicurezza nazionale, protezione dei dati e governance dell'IA. Il percorso è iniziato nel 2017 con la Cybersecurity Law, per poi articolarsi attraverso i Beijing AI Principles e i principi sullo sviluppo

responsabile della nuova generazione di intelligenza artificiale, entrambi pubblicati nel 2019, fino alle più recenti misure provvisorie per la gestione dei servizi di IA generativa, in vigore dall'agosto 2023. A questo si affianca un impianto di protezione dei dati personali strutturato attorno a tre pilastri normativi paralleli, e un'iniziativa strategica come la Borsa dei dati di Shanghai, pensata per creare un modello di riferimento globale nella compravendita di dati e ridurre l'incertezza giuridica che oggi ostacola la loro circolazione.

1.2 La strategia europea: dalla tecnologia alle regole

Il concetto di "sovranità digitale europea", evocato dalla Presidente della Commissione europea fin dal discorso sullo stato dell'Unione del 2020, sintetizza bene l'ambizione politica sottostante alla strategia normativa di Bruxelles. Si tratta, va sottolineato, di un'affermazione di natura politica più che giuridica: descrive un obiettivo da raggiungere, non uno stato di fatto già consolidato. L'Europa non possiede una leadership tecnologica nel campo dell'IA, non essendo tra i principali produttori mondiali; ciò che persegue, piuttosto, è la capacità di utilizzare i propri strumenti regolatori per plasmare standard di portata globale, secondo la logica del cosiddetto "effetto Bruxelles" — la stessa dinamica per cui regole adottate in sede europea finiscono per essere recepite, de facto o de iure, anche in altre giurisdizioni.

Questa strategia si inserisce in un disegno più ampio, che mira alla costruzione di un mercato unico digitale europeo attraverso quattro pilastri normativi interconnessi: la disciplina della protezione e valorizzazione dei dati personali (con il GDPR e i regolamenti complementari su dati, governance dei dati e spazio sanitario europeo); la regolazione dei mercati e servizi digitali (con il Digital Markets Act e il Digital Services Act); l'identità digitale (con la revisione del regolamento eIDAS); e, infine, l'intelligenza artificiale, disciplinata dall'AI Act e affiancata dalla proposta di direttiva sulla responsabilità civile da IA.

Un elemento tecnico ma politicamente significativo riguarda l'ambito di applicazione territoriale del Regolamento, costruito sul modello già sperimentato dal GDPR: l'AI Act si applica non solo ai soggetti stabiliti nell'Unione, ma anche a fornitori e utilizzatori situati in paesi terzi, ogniqualvolta l'output del sistema di IA sia destinato a essere utilizzato nel territorio europeo. Questa estensione extraterritoriale rappresenta lo strumento attraverso cui l'Unione cerca di trasformare la propria

normazione interna in un punto di riferimento globale, proteggendo al contempo non solo i diritti fondamentali ma anche i "valori" europei, espressione che ricorre frequentemente nei testi preparatori e che segnala l'ambizione di un modello non solo giuridico, ma anche culturale.

Va infine segnalato, come elemento di contesto storico recente, che la guerra in Ucraina ha contribuito a rafforzare il ruolo degli stati nazionali nel governo del digitale, in particolare per ragioni di sicurezza cibernetica: un fenomeno che si affianca, senza necessariamente contraddirlo, al disegno di armonizzazione sovranazionale perseguito dall'Unione.

2. L'architettura dell'AI Act: un regolamento basato sul rischio

2.1 Obiettivi, struttura e definizione di sistema di IA

Il Regolamento europeo sull'intelligenza artificiale adotta un approccio orizzontale: disciplina l'IA come fenomeno generale, senza limitarsi a settori specifici, sebbene il Parlamento europeo abbia successivamente adottato risoluzioni mirate su aspetti particolari come l'etica, la responsabilità e il diritto d'autore. L'obiettivo dichiarato è duplice: fare dell'Unione europea un leader mondiale nello sviluppo di un'IA sicura, affidabile ed etica, e al contempo preservarne la competitività tecnologica in un settore in cui, come visto, l'Europa non occupa una posizione di vertice.

Gli obiettivi specifici del Regolamento includono: garantire che i sistemi di IA immessi sul mercato europeo siano sicuri e rispettino i diritti fondamentali; assicurare certezza del diritto per favorire investimenti e innovazione; rafforzare la governance e l'applicazione effettiva della normativa esistente; e facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite e affidabili, prevenendo la frammentazione normativa tra stati membri.

Dal punto di vista dimensionale, il testo finale del Regolamento testimonia la complessità della materia: la proposta iniziale di 85 articoli si è progressivamente ampliata fino a raggiungere 113 articoli, 180 considerando e 13 allegati. La definizione di sistema di intelligenza artificiale adottata è volutamente ampia: un sistema automatizzato progettato per operare con livelli di autonomia variabili, capace di adattarsi dopo la diffusione e di dedurre, da input ricevuti e per obiettivi espliciti o impliciti, output quali previsioni, contenuti, raccomandazioni o decisioni in grado di influenzare ambienti fisici o virtuali. Una definizione così onnicomprensiva consente di applicare il

Regolamento a una gamma estremamente eterogenea di tecnologie, ma pone — come si vedrà — anche alcuni problemi.

2.2 Le quattro categorie di rischio e le pratiche vietate

Il cuore metodologico dell'AI Act è la classificazione dei sistemi di IA in quattro categorie di rischio: inaccettabile, alto, opacità e basso o minimo. A ciascuna categoria corrisponde un regime giuridico differenziato, che va dal divieto assoluto per i sistemi a rischio inaccettabile, fino a un regime di utilizzo libero per quelli a rischio minimo, passando per obblighi di trasparenza per i sistemi a rischio di opacità e un articolato sistema di conformità per quelli ad alto rischio (già anticipati nel secondo capitolo di questo documento).

Tra le pratiche espressamente vietate figurano l'uso di tecniche subliminali e lo sfruttamento delle vulnerabilità di specifici gruppi di persone, quando tali pratiche siano finalizzate a distorcere materialmente il comportamento di un individuo o a provocare un danno significativo. Sono altresì proibiti i sistemi di punteggio sociale lesivi della dignità umana e, salvo eccezioni circoscritte — come la ricerca mirata di vittime di tratta o sfruttamento sessuale — l'identificazione biometrica remota in tempo reale in spazi pubblici per finalità di contrasto alla criminalità.

La categoria dei sistemi ad alto rischio è particolarmente estesa e comprende, tra l'altro, i sistemi di identificazione biometrica remota, quelli impiegati come componenti di sicurezza nella gestione del traffico o nelle infrastrutture critiche (acqua, gas, energia elettrica), i sistemi utilizzati per l'accesso all'istruzione, per la selezione e gestione del personale (assunzione, promozione, cessazione del rapporto, monitoraggio delle prestazioni), per la valutazione dell'affidabilità creditizia, per la gestione delle chiamate di emergenza, per il supporto alle autorità di contrasto nella valutazione delle prove, e per l'assistenza alle autorità giudiziarie nell'interpretazione dei fatti e del diritto. Anche i sistemi impiegati nelle procedure di immigrazione, asilo e controllo delle frontiere rientrano in questa categoria.

Un elemento di flessibilità è rappresentato dalla possibilità, per il fornitore stesso, di valutare che un sistema elencato non comporti in realtà un rischio significativo per la salute, la sicurezza o i diritti fondamentali — fatta salva la previsione che i sistemi che effettuano profilazione di persone

fisiche siano sempre considerati ad alto rischio. Tale autovalutazione deve essere documentata prima dell'immissione sul mercato e resa disponibile alle autorità competenti su richiesta.

2.3 Gli obblighi per i sistemi ad alto rischio e per i modelli generativi

Per i sistemi classificati ad alto rischio, il Regolamento prevede un impianto di compliance articolato. In primo luogo, è richiesta l'istituzione di un sistema di gestione del rischio inteso come processo iterativo continuo, da mantenere lungo tutto il ciclo di vita del sistema, che comprenda l'identificazione, la stima e la valutazione dei rischi noti e ragionevolmente prevedibili, incluso il monitoraggio successivo all'immissione sul mercato.

A questo si affiancano requisiti di qualità per i set di dati utilizzati nell'addestramento, nella convalida e nel collaudo — che devono essere pertinenti, rappresentativi e, nella misura del possibile, esenti da errori — l'obbligo di predisporre una documentazione tecnica completa prima dell'immissione sul mercato, meccanismi di registrazione automatica degli eventi per garantire la tracciabilità del funzionamento, istruzioni per l'uso chiare e accessibili, interfacce che consentano un'efficace supervisione umana, e infine standard adeguati di accuratezza, robustezza e cybersicurezza per l'intero ciclo di vita del sistema. Alcuni soggetti della filiera, tra cui taluni enti pubblici e gli utilizzatori di sistemi particolarmente sensibili come quelli per la valutazione del credito, sono inoltre tenuti a condurre una valutazione d'impatto sui diritti fondamentali.

Anche i sistemi non classificati ad alto rischio, ma che presentano rischi di opacità, sono soggetti a obblighi minimi di trasparenza: i sistemi destinati a interagire direttamente con le persone devono segnalare la natura artificiale dell'interazione, salvo che ciò risulti già evidente dal contesto; i sistemi di riconoscimento delle emozioni o categorizzazione biometrica devono informare gli utenti del proprio funzionamento; i contenuti generati artificialmente che simulano persone, oggetti o eventi reali — i cosiddetti deepfake — devono essere riconoscibili come tali.

Una novità significativa, introdotta successivamente alla proposta originaria in risposta all'emergere di modelli come ChatGPT, riguarda la disciplina dei "modelli di IA per finalità generali" (i foundation model). Anche in questo caso il legislatore adotta una logica basata sul rischio: i modelli che non comportano un rischio sistemico sono soggetti a obblighi relativamente contenuti,

quali il rispetto della normativa sul diritto d'autore e la redazione di sintesi sui contenuti utilizzati per l'addestramento; quelli che invece presentano un rischio sistemico devono attenuare i rischi identificati, notificare gli incidenti gravi all'Ufficio europeo per l'IA e garantire un adeguato livello di cybersicurezza, sia del modello che della sua infrastruttura fisica.

3. Le criticità del modello europeo

3.1 Rigidità temporale e indifferenziazione degli obblighi

Pur riconoscendo il valore dello sforzo regolatorio compiuto dall'Unione europea — prima giurisdizione al mondo a tentare una disciplina organica e generale dell'intelligenza artificiale — è inevitabile rilevare alcune criticità strutturali del modello adottato.

Una prima debolezza riguarda la rigidità intrinseca della classificazione per categorie di rischio. Trattandosi di un elenco normativo predefinito, esso è destinato a essere costantemente superato dall'evoluzione tecnologica: lo stesso processo di approvazione del Regolamento ha dovuto essere interrotto e rivisto per includere l'intelligenza artificiale generativa e i modelli fondazionali, fenomeni emersi successivamente alla proposta originaria. Questo precedente segnala un limite strutturale: un sistema normativo costruito sulla fotografia tecnologica del presente fatica intrinsecamente a restare aggiornato rispetto a sviluppi futuri non ancora prevedibili.

Un confronto istruttivo si può fare con il GDPR, altro grande esempio di regolazione basata sulla gestione del rischio adottato dal legislatore europeo. La differenza sostanziale sta nel fatto che nel GDPR il principio di accountability pone in capo al titolare del trattamento la responsabilità di valutare e gestire dinamicamente il rischio, consentendo un adattamento continuo alle caratteristiche specifiche di ciascun trattamento. Nell'AI Act, al contrario, è il legislatore stesso a predeterminare quali sistemi siano ad alto rischio e come tale rischio debba essere affrontato, partendo peraltro da una definizione di sistema di IA estremamente ampia. Questo approccio “top down” rischia di rivelarsi meno adattivo rispetto a un modello che responsabilizzi gli operatori nella valutazione continua dei rischi specifici delle proprie applicazioni.

Una seconda criticità deriva dall'imposizione dei medesimi obblighi a tutti gli operatori, indipendentemente dalle dimensioni dell'impresa e dall'effettiva criticità dell'attività svolta. Questo

approccio indifferenziato comporta oneri amministrativi rilevanti — redazione di piani di gestione del rischio, certificazioni, notifiche, documentazione tecnica, marcature di conformità — che gravano in modo sostanzialmente uguale su una grande corporation e su una piccola startup. Mentre le imprese di grandi dimensioni dispongono tipicamente delle risorse per assorbire questi costi di compliance, le piccole e medie imprese, le startup e il mondo della ricerca — particolarmente rilevanti nel contesto produttivo italiano — rischiano di subire un impatto economico sproporzionato. Il legislatore europeo demanda agli stati membri il compito di mitigare questo squilibrio attraverso spazi di sperimentazione normativa (i cosiddetti sand-box regolatori) e misure di sostegno dedicate alle PMI, ma resta il fatto che l'impianto di base non distingue adeguatamente in funzione della scala e del contesto applicativo.

3.2 Il rischio di burocratizzazione senza un correlato aumento di tutela

La terza criticità, forse la più rilevante dal punto di vista sostanziale, riguarda il rischio che l'impianto regolatorio si traduca in una burocratizzazione del mercato europeo dell'IA senza generare un proporzionale incremento della tutela effettiva dei diritti. Il Regolamento prescrive un numero considerevole di obblighi formali — orientati principalmente al conseguimento della certificazione di conformità — ma la domanda sostanziale che resta aperta è se questo apparato sia davvero in grado di rispondere ai pericoli concreti, dalla discriminazione algoritmica alla manipolazione, che hanno motivato l'intervento normativo.

Gli strumenti di tutela individuale previsti dal Regolamento sono, in fin dei conti, piuttosto limitati: il diritto di presentare reclamo all'autorità di vigilanza del mercato e il diritto a una spiegazione dei processi decisionali. Per il resto, ci si appoggia agli strumenti già previsti dal GDPR — diritto di accesso, diritto di cancellazione, diritto alla portabilità dei dati — e ai principi sostanziali ad esso collegati, quali qualità, esattezza e minimizzazione dei dati. Non si rinvengono, in altri termini, strumenti di tutela individuale o collettiva realmente nuovi e specificamente calibrati sulle peculiarità dell'intelligenza artificiale.

Particolarmente significativo è il rinvio della questione più delicata, quella della costruzione di un nuovo modello di responsabilità civile per i danni causati dai sistemi di IA. La Commissione europea aveva inizialmente ipotizzato persino la possibilità di una soggettività giuridica per le applicazioni

di intelligenza artificiale; nel testo finale del Regolamento, tuttavia, ci si limita a richiedere che il fornitore di un sistema ad alto rischio garantisca la conformità ai requisiti previsti. La proposta di direttiva sulla responsabilità da IA, dal suo lato, segue un approccio di armonizzazione minima, lasciando ampi margini di discrezionalità agli stati membri.

Nel complesso, il Regolamento si configura essenzialmente come una cornice amministrativa per l'immissione sul mercato dei prodotti di IA, il cui contenuto sostanziale dovrà essere completato da atti delegati, norme tecniche e standard — strumenti che assumeranno un'importanza decisiva nella concreta applicazione del sistema, ma che restano, per ora, ampiamente da definire.

4. Oltre la forma: le questioni sostanziali ancora aperte

4.1 Responsabilità, dati e tutela contro la discriminazione

Se l'Unione europea intende davvero affermarsi come modello di riferimento globale per la regolazione dell'intelligenza artificiale, e non limitarsi a una funzione meramente organizzativa e certificativa, è necessario che alcune questioni sostanziali — finora rinviate o trattate solo in modo parziale — vengano affrontate con maggiore determinazione.

La prima riguarda la definizione di un modello generale di responsabilità per i danni causati dalle applicazioni di intelligenza artificiale, che vada oltre l'approccio di armonizzazione minima oggi adottato. Si tratta di un nodo cruciale: l'allocazione della responsabilità tra fornitore, deployer e, in alcuni casi, utilizzatore finale, condiziona direttamente l'effettività della tutela per chi subisce un danno derivante dal funzionamento di un sistema di IA.

La seconda questione riguarda l'elaborazione di soluzioni giuridiche capaci di consentire, nel pieno rispetto dei diritti fondamentali, un flusso adeguato di dati personali e non personali verso le applicazioni di intelligenza artificiale. L'addestramento di sistemi efficaci richiede grandi quantità di dati di qualità, e un equilibrio normativo che blocchi eccessivamente questo flusso rischia di compromettere proprio quella competitività che l'Unione dichiara di voler promuovere.

La terza priorità riguarda l'individuazione di strumenti di tutela contro la discriminazione che siano realmente efficaci e rapidi, andando oltre i meccanismi di reclamo amministrativo e le tutele

mutuate dal GDPR. Si tratta di un ambito in cui la specificità dei sistemi di IA — la loro opacità, la scala di applicazione, la difficoltà di individuare il nesso causale tra funzionamento del sistema e danno discriminatorio subito — richiederebbe strumenti procedurali nuovi, calibrati sulle caratteristiche di queste tecnologie.

4.2 Tra affermazione del modello e rischio di isolamento

Un ultimo ordine di considerazioni riguarda la dimensione internazionale della strategia regolatoria europea. È legittimo e per certi versi necessario che l'Unione europea proponga e affermi un proprio modello normativo, replicando una strategia già adottata con successo in altri ambiti del diritto digitale. Tuttavia, altrettanto importante è evitare che questa affermazione si traduca in un isolamento dell'Europa rispetto al resto del mondo.

Il momento storico attuale presenta, da questo punto di vista, un'opportunità non scontata: sia gli Stati Uniti che la Cina sembrano orientarsi, pur partendo da premesse e modelli istituzionali molto diversi, su principi che non risultano poi così distanti da quelli europei in materia di sicurezza, trasparenza e affidabilità dei sistemi di IA. Questa convergenza, per quanto parziale, apre uno spazio di possibile cooperazione normativa internazionale che l'Unione europea farebbe bene a coltivare attivamente, anziché limitarsi a esportare unilateralmente il proprio modello.

La metafora delle fortezze e dei ponti sintetizza efficacemente questa esigenza: costruire un proprio sistema di regole solide e coerenti è legittimo e per certi versi indispensabile, ma occorre contestualmente costruire anche i canali di dialogo e cooperazione che consentano l'interoperabilità con gli altri grandi sistemi regolatori globali. Solo un equilibrio tra affermazione del modello europeo e apertura alla cooperazione internazionale può evitare che la regolazione, da strumento di leadership, si trasformi in un fattore di marginalizzazione del continente nel più ampio scenario geopolitico dell'intelligenza artificiale.

5. Considerazioni di sintesi

Il percorso regolatorio europeo sull'intelligenza artificiale rappresenta un tentativo pionieristico di costruire una disciplina organica per una tecnologia trasversale e in rapidissima evoluzione. Il merito di aver affrontato la materia con un approccio sistemico, fondato sulla classificazione del rischio, va riconosciuto, così come l'ambizione di porre al centro la tutela dei diritti fondamentali e dei valori europei.

Tuttavia, l'analisi delle criticità evidenzia come il modello presenti margini di miglioramento non trascurabili: la rigidità di una classificazione normativa predefinita rispetto a una tecnologia in costante mutamento; l'imposizione di obblighi sostanzialmente omogenei a soggetti di scala e capacità molto diverse tra loro; e il rischio, non meramente teorico, che l'apparato di compliance produca burocratizzazione senza un proporzionale incremento della tutela sostanziale dei diritti delle persone.

La sfida che attende il legislatore europeo nei prossimi anni non riguarda quindi tanto l'affinamento tecnico dell'impianto già adottato, quanto l'affrontare con determinazione le questioni sostanziali rimaste sullo sfondo: un modello di responsabilità civile realmente adeguato alle peculiarità dell'IA, soluzioni giuridiche equilibrate per la circolazione dei dati necessari all'addestramento dei sistemi, e strumenti di tutela contro la discriminazione che siano concretamente efficaci. A questo si affianca la necessità — non meno strategica — di evitare che l'affermazione di un modello regolatorio europeo si traduca in un isolamento del continente, privilegiando invece la costruzione di ponti di cooperazione normativa con le altre grandi aree geopolitiche, in un momento storico che offre margini di convergenza non scontati.

Capitolo 5 – La cybersecurity ai tempi dell'AI

1. Un'escalation senza precedenti: il panorama della minaccia cyber

1.1 La traiettoria degli attacchi in Italia e nel mondo

Il rischio informatico ha smesso da tempo di essere un fenomeno marginale o settoriale. I dati più recenti dipingono un quadro in costante deterioramento: a livello globale, il numero di attacchi portati a termine è cresciuto di circa il 60% nel quinquennio 2019-2023, con una composizione sempre più spostata verso episodi classificati ad alto impatto. La tendenza è particolarmente marcata in Italia, dove la velocità di crescita degli attacchi supera la media internazionale in misura significativa.

L'Italia si colloca al settimo posto mondiale per numero di incidenti informatici subiti, una posizione che stride con il peso economico del Paese. Questo dato non è casuale: la struttura produttiva italiana, caratterizzata da un tessuto di quasi un milione di operatori tra piccole imprese e studi professionali, rappresenta un ambiente particolarmente favorevole per i cyber criminali. Le limitate competenze tecniche interne e la scarsa disponibilità finanziaria da destinare alla sicurezza informatica rendono le piccole e medie imprese bersagli privilegiati, perché più vulnerabili e, paradossalmente, più inclini a cedere alle richieste estorsive.

Le PMI tendono infatti a vedere nel pagamento del riscatto una via d'uscita rapida, capace di ridurre i tempi di interruzione operativa e di preservare le relazioni commerciali. Questa logica non è irrazionale dal punto di vista della singola impresa, ma alimenta un ecosistema criminale sempre più strutturato e redditizio. Le conseguenze di un attacco informatico per una PMI possono essere devastanti: la perdita totale dei dati relativi a clienti, fornitori e ordini. Alcune stime — peraltro non unanimemente condivise dalla comunità scientifica — ipotizzano che più della metà delle PMI vittime di un attacco cyber rischi concretamente il fallimento.

1.2 Il recepimento della direttiva NIS2 nell'ordinamento italiano

In questo contesto si inserisce il recepimento italiano della direttiva europea 2022/2555, nota come NIS2, tramite il D.Lgs. 138/2024. La direttiva segna una discontinuità significativa rispetto al quadro normativo precedente: se le norme previgenti concentravano gli obblighi di sicurezza su poche centinaia di soggetti ritenuti critici per il sistema-Paese, il nuovo impianto allarga drasticamente la platea dei destinatari. Si stima che tra 50.000 e 80.000 aziende italiane saranno soggette agli obblighi NIS2, in quanto operanti in uno dei diciassette settori individuati come essenziali o importanti.

I settori coinvolti coprono l'intera dorsale dell'economia moderna: dall'energia ai trasporti, dal settore bancario alle infrastrutture digitali, dalla sanità alla pubblica amministrazione, fino alla produzione di macchinari, dispositivi medici ed elettronici. La logica sottostante riconosce che le interdipendenze tra settori rendono ogni anello debole della catena un potenziale punto di ingresso per attacchi con effetti a cascata ben oltre il perimetro del soggetto colpito.

Gli obblighi introdotti dalla NIS2 sono articolati e richiedono uno sforzo organizzativo non banale. Le imprese sono chiamate ad adottare misure tecniche, operative e organizzative proporzionate al proprio livello di rischio. Tra le prescrizioni più rilevanti figurano: la conduzione periodica di analisi dei rischi informatici, il possesso di procedure strutturate per la gestione degli incidenti, l'implementazione di piani di backup e disaster recovery, la protezione della catena di approvvigionamento, la formazione del personale in materia di igiene informatica e l'adozione di sistemi di autenticazione a più fattori.

Sul fronte della notifica degli incidenti, la direttiva stabilisce tempi stringenti: un preallarme al CSIRT entro 24 ore dalla scoperta dell'incidente significativo, seguito da una notifica formale entro 72 ore, contenente una valutazione iniziale della gravità e dell'impatto, comprensivi di indicatori di compromissione e stima degli effetti transfrontalieri. Un aspetto che mette ulteriormente sotto pressione le strutture organizzative delle imprese meno attrezzate.

Il problema di fondo è la scarsità di competenze. Il World Economic Forum stima un deficit globale di circa quattro milioni di professionisti della cybersecurity; per il solo territorio italiano la carenza si aggirerebbe intorno alle centomila unità. In un simile contesto, l'intelligenza artificiale è

chiamata a svolgere un ruolo compensativo, supportando le organizzazioni nelle fasi di raccolta e analisi preliminare delle informazioni e nell'orientamento verso le soluzioni più appropriate.

2. L'anatomia del cybercrime contemporaneo

2.1 Il modello crime-as-a-service e la professionalizzazione dei criminali

Uno degli aspetti più rilevanti e meno intuitivi del panorama della minaccia cyber riguarda la natura dei soggetti che la generano. L'immagine stereotipata del hacker solitario, rinchiuso in uno scantinato, appartiene alla narrativa popolare ma non alla realtà operativa del cybercrime contemporaneo. I gruppi che oggi costituiscono la principale fonte di rischio per le organizzazioni sono strutture altamente organizzate, con modelli gestionali che ricordano quelli delle imprese commerciali più che quelli delle associazioni criminali tradizionali.

Il paradigma dominante è quello del crime-as-a-service (CaaS), un modello in cui diversi attori specializzati cooperano in modo quasi contrattuale per massimizzare l'efficacia degli attacchi e la redditività delle operazioni estorsive. Lo schema si articola tipicamente su tre livelli funzionali distinti. Al primo livello si trovano gli sviluppatori di ransomware, che creano e gestiscono il malware, curano le infrastrutture di pagamento e si occupano della comunicazione con le vittime. Al secondo livello operano gli Initial Access Brokers (IAB), specializzati nell'identificare organizzazioni vulnerabili, raccogliere credenziali compromesse e condurre campagne di phishing mirato per poi rivendere gli accessi ottenuti sui mercati del dark web. Al terzo livello agiscono gli affiliati, che acquistano queste informazioni e le utilizzano per scatenare gli attacchi effettivi, avvalendosi degli strumenti messi a disposizione dai proprietari del ransomware.

Le modalità operative di gruppi come Lockbit 3.0 mostrano una sofisticazione che si estende anche alle strategie di customer care nei confronti delle vittime: opzioni multiple di pagamento, dilazioni nei tempi di decisione, offerte di sola distruzione dei dati esfiltrati, persino programmi di bug bounty per segnalare vulnerabilità nel proprio codice. I materiali trapelati nel caso del gruppo Conti — reso pubblico nel contesto del conflitto russo-ucraino — hanno offerto uno spaccato raro sulle dinamiche interne di queste organizzazioni: sistemi di incentivazione, piani di carriera per i membri, allocazione strategica di risorse finanziarie e umane. Sorprendentemente, molti affiliati

erano professionisti che operavano nell'economia legale e integravano i propri redditi partecipando alle attività criminali a latere.

2.2 L'intelligenza artificiale come moltiplicatore della capacità offensiva

L'intelligenza artificiale non è uno strumento neutro nel contesto della sicurezza informatica: viene ampiamente adottata anche dagli attaccanti per amplificare l'efficacia e la scala delle proprie operazioni. L'esempio più diffuso riguarda l'evoluzione delle campagne di phishing. Fino a qualche anno fa, le email fraudolente erano spesso riconoscibili per la grammatica approssimativa, l'assenza di contestualizzazione e il mittente incongruente. L'adozione di strumenti di IA generativa ha trasformato queste tecniche: oggi le campagne di spear phishing producono messaggi grammaticalmente corretti, personalizzati sulla base delle informazioni digitali lasciate dalle vittime su social network e altre piattaforme, costruiti per sfruttare contesti, interessi e relazioni specifiche del destinatario. Strumenti capaci di raccogliere e sintetizzare automaticamente queste informazioni sono disponibili non solo nel dark web, ma anche in ambienti accessibili al pubblico generale.

Un secondo ambito di applicazione riguarda lo sviluppo automatizzato di malware. L'IA consente di ridurre i tempi di creazione e di migliorare la qualità del codice malevolo, abbassando le barriere d'ingresso per nuovi attori e accelerando il ciclo di aggiornamento degli strumenti di attacco. Ma la frontiera più insidiosa è rappresentata dai deepfake: la manipolazione di audio, video e immagini per far apparire che una persona dica o faccia qualcosa che non ha mai detto o fatto. Il caso della filiale hongkonghese di una società britannica, dove un dipendente ha autorizzato un trasferimento di 25 milioni di dollari convinto di aver ricevuto istruzioni via videochiamata dal proprio superiore — che in realtà era un deepfake — illustra in modo emblematico la portata di questa minaccia.

Al vertice della scala di sofisticazione si collocano gli attacchi APT (Advanced Persistent Threat), tipicamente condotti da soggetti sponsorizzati da stati nazionali. Una volta ottenuto accesso a una rete, questi attaccanti utilizzano algoritmi di IA per muoversi lateralmente in modo silenzioso, studiare il comportamento dell'infrastruttura, identificare i punti di esfiltrazione più efficaci e creare backdoor difficili da rilevare. La combinazione di persistenza, sofisticazione tecnica e risorse

statali rende gli APT una minaccia qualitativamente diversa rispetto al cybercrime ordinario, con impatti potenziali di lungo periodo su sicurezza nazionale e competitività economica.

3. Verso una valutazione dinamica del rischio cyber

3.1 I limiti degli approcci tradizionali alla gestione del rischio

Il rischio, inteso in senso generale come prodotto di probabilità e impatto di un evento avverso, assume nel dominio della cybersecurity caratteristiche specifiche che ne complicano la misurazione e la gestione. La probabilità di un incidente informatico non dipende solo da fattori tecnici interni all'organizzazione, ma anche dalla sua attrattività come obiettivo, dal numero e dalla gravità delle vulnerabilità presenti nei sistemi, e dalla presenza di attori minacciosi motivati a sfruttarle. L'impatto, a sua volta, si misura in termini di compromissione della riservatezza, dell'integrità e della disponibilità di dati e servizi, con ricadute economiche, reputazionali e operative.

I metodi di analisi del rischio tradizionali — tra cui ISO/IEC 27005, il framework NIST RMF, COBIT e OCTAVE — presentano limiti strutturali che li rendono sempre meno adeguati a fronteggiare un panorama di minacce in rapida evoluzione. Il problema fondamentale è la loro natura statica: fotografano la postura di sicurezza di un'organizzazione in un momento determinato, senza la capacità di aggiornarsi automaticamente al mutare delle condizioni. Non sono in grado di incorporare in tempo reale le informazioni provenienti da nuovi database di vulnerabilità, non reagiscono all'emergere di nuove tipologie di attacco come gli zero-day, e non modellano adeguatamente le modifiche architetturali introdotte dall'adozione di infrastrutture cloud, dispositivi IoT o soluzioni basate sull'IA stessa — che, paradossalmente, ampliano la superficie di attacco mentre migliorano l'efficienza operativa.

3.2 Le reti bayesiane come strumento di valutazione dinamica

Per superare questi limiti, la letteratura recente indica nelle reti bayesiane uno strumento particolarmente promettente. Si tratta di modelli probabilistici grafici che rappresentano le relazioni di causalità tra variabili rilevanti per la sicurezza — vulnerabilità, minacce, asset, stati di

sicurezza dei sistemi — assegnando a ciascun nodo una probabilità condizionale di attivazione. La loro caratteristica principale è la capacità di aggiornarsi dinamicamente: man mano che nuove informazioni diventano disponibili — una nuova vulnerabilità scoperta, l'emergere di un nuovo gruppo minaccioso, l'identificazione di un'anomalia nel traffico di rete — le probabilità associate ai nodi vengono ricalcolate, aggiornando in tempo reale la valutazione complessiva del rischio.

Le reti bayesiane permettono inoltre di modellare le interdipendenze tra componenti dell'infrastruttura aziendale, catturando i potenziali effetti a cascata di un attacco che compromette un singolo elemento: non solo il danno diretto sul componente colpito, ma la propagazione del rischio ad altri sistemi e linee di business. Questa proprietà le rende particolarmente utili per simulare scenari ipotetici — stimare, ad esempio, il danno potenziale di un attacco ransomware in diverse condizioni, o confrontare l'efficacia di diverse strategie di mitigazione — consentendo di prioritizzare le azioni di difesa in modo informato e proporzionato alla criticità dei rischi.

Un sistema di valutazione del rischio basato su reti bayesiane dovrebbe idealmente integrare quattro capacità fondamentali: adattarsi automaticamente ai cambiamenti infrastrutturali (nuovi servizi cloud, nuovi dispositivi); incorporare in tempo reale le informazioni provenienti da database di vulnerabilità come il National Vulnerability Database (NVD) gestito dal NIST; integrare flussi di monitoraggio continuo capaci di rilevare anomalie comportamentali; prioritizzare dinamicamente i rischi per concentrare le risorse sulle minacce più imminenti e critiche.

4. L'IA a supporto della gestione degli incidenti: il caso PACY

4.1 Il gap di sicurezza nelle piccole e medie imprese

Le PMI occupano una posizione paradossale nel panorama della cybersecurity: costituiscono la spina dorsale dell'economia europea — rappresentando il 90% delle imprese e fornendo due terzi dell'occupazione del settore privato, secondo i dati dell'Organizzazione Mondiale del Commercio — ma sono allo stesso tempo le organizzazioni meno attrezzate per far fronte alle minacce informatiche. La combinazione di scarsa consapevolezza dei rischi, risorse finanziarie limitate e assenza di competenze tecniche interne crea un circolo vizioso: la sottovalutazione del rischio porta

a sottoinvestimenti nella sicurezza, che a loro volta aumentano l'esposizione alle minacce, che in caso di incidente possono rivelarsi fatali per la sopravvivenza stessa dell'impresa.

Questa vulnerabilità strutturale si scontra con un contesto normativo che, con la NIS2, chiede proprio alle PMI di fare un salto qualitativo in termini di capacità di gestione della sicurezza. Gli standard internazionali esistenti per la gestione degli incidenti (ISO, NIST, COBIT, PCI DSS) sono stati concepiti per organizzazioni strutturate, dotate di team dedicati alla sicurezza, di budget adeguati e di competenze legali e comunicative per navigare le complessità normative. Per una PMI, la sola comprensione e selezione degli standard applicabili al proprio settore rappresenta già un ostacolo significativo, prima ancora di passare all'implementazione.

Il Cybersecurity Framework del NIST identifica cinque funzioni fondamentali per la corretta gestione degli incidenti: identificare, proteggere, rilevare, rispondere e recuperare. Ciascuna di queste dimensioni richiede competenze specifiche che raramente sono disponibili internamente nelle piccole imprese. E quando si verifica un incidente, i tempi di risposta diventano critici: ogni ora di inattività, ogni dato perso, ogni relazione commerciale compromessa ha un costo che può essere determinante per la sopravvivenza dell'impresa.

4.2 Il progetto PACY: architettura e funzionalità

In questo contesto si colloca il progetto Pro-Active Cyber Security (PACY), sviluppato dall'Università Campus Bio-Medico di Roma con il supporto di un finanziamento Google. PACY si propone di realizzare una piattaforma accessibile e intuitiva che, attraverso l'utilizzo dell'intelligenza artificiale generativa, supporti le PMI nella gestione degli incidenti informatici, colmando il gap di competenze e risorse che le affligge strutturalmente.

Il cuore tecnologico della piattaforma è Gemini, il large language model (LLM) di Google, orchestrato attraverso una logica ad agenti. I prompt sono stati ingegnerizzati integrando conoscenze qualificate provenienti da numerose interviste con esperti del settore — tra cui rappresentanti della Polizia Postale e dei Carabinieri — e calibrati rispetto alle esigenze concrete delle PMI in termini di semplicità del linguaggio e facilità di interazione. L'obiettivo dichiarato è rendere la piattaforma utilizzabile da personale senza formazione tecnica specializzata.

L'architettura del sistema si basa su una molteplicità di agenti specializzati, coordinati da un agente di triage il cui compito è instradare la richiesta dell'utente verso l'agente più adatto in base al tipo di incidente descritto. L'interazione avviene in linguaggio naturale: l'utente descrive i sintomi del problema informatico e il sistema guida la diagnosi attraverso domande strutturate, fornendo risposte tecniche immediate (ad esempio, disconnettere i dispositivi infetti dalla rete), indicazioni sulle autorità competenti da contattare e supporto nella predisposizione delle notifiche obbligatorie previste dalla normativa.

Una funzionalità particolarmente rilevante è la generazione automatica di report tecnici sugli incidenti, che includono la descrizione delle vulnerabilità sfruttate, l'impatto sui sistemi aziendali, informazioni utili per le eventuali indagini delle forze dell'ordine o del Garante della Privacy, e raccomandazioni operative per la mitigazione del danno e il miglioramento della sicurezza futura. Questi report rispondono direttamente ai requisiti di notifica previsti dalla NIS2, semplificando un processo che per molte PMI sarebbe altrimenti inaccessibile.

A partire dalle informazioni fornite dall'azienda in fase di registrazione, la piattaforma svolge anche una funzione di monitoraggio proattivo: notifica all'utente se la sua azienda o i suoi fornitori sono stati attaccati da gruppi ransomware noti, se il settore di appartenenza è sotto pressione, o se un determinato gruppo criminale è particolarmente attivo nel territorio di riferimento. Questa capacità di contestualizzazione trasforma PACY da strumento reattivo a presidio di sicurezza continuativo.

La piattaforma integra inoltre VirusTotal, il servizio di analisi di file e URL sospetti che aggrega le valutazioni di numerosi motori antivirus. Gli utenti possono caricare file o inviare link direttamente nell'interfaccia del chatbot per ricevere un'analisi immediata del rischio, con indicazione del numero di motori di rilevamento che segnalano il file come malevolo e dettagli sui problemi identificati. Questa integrazione abbassa ulteriormente la barriera tecnica per l'utente finale, che non deve accedere a strumenti separati o interpretare output tecnici complessi.

5. Riflessioni conclusive e prospettive

5.1 Un ecosistema in trasformazione permanente

Il panorama della cybersecurity è oggi caratterizzato da una dinamica di trasformazione permanente che rende obsolete con rapidità crescente sia le tecnologie difensive che i quadri normativi. La minaccia evolve lungo due assi principali: la frequenza degli attacchi è in aumento costante, ma è la sofisticazione a rappresentare la sfida più insidiosa. La professionalizzazione dei gruppi criminali, la disponibilità di strumenti basati sull'IA per automatizzare e personalizzare gli attacchi, e l'adozione di modelli organizzativi mutuati dal mondo delle imprese legali rendono il cybercrime contemporaneo un avversario di qualità radicalmente diversa rispetto al passato.

In questo contesto, la direttiva NIS2 rappresenta un tentativo di sistematizzare la risposta a livello europeo, imponendo standard minimi di sicurezza a una platea molto più ampia di soggetti. Si tratta di un passo necessario, ma che porta con sé sfide implementative concrete, soprattutto per le organizzazioni meno strutturate. La normativa chiede alle PMI di adottare pratiche e procedure che presuppongono competenze e risorse che spesso non possiedono, creando un potenziale divario tra obiettivo regolatorio e capacità di conformità effettiva.

5.2 L'IA come risorsa strategica per la difesa

L'intelligenza artificiale emerge come risposta trasversale a molte delle sfide descritte. Sul versante della valutazione del rischio, i modelli probabilistici dinamici — in primo luogo le reti bayesiane — consentono un approccio alla sicurezza informatica che non è più un'istantanea periodica ma un processo continuo di aggiornamento. Sul versante della risposta agli incidenti, sistemi come PACY dimostrano che l'IA generativa può fungere da amplificatore di competenze, rendendo accessibili a organizzazioni non specializzate capacità di diagnosi, gestione e reportistica che altrimenti richiederebbero team dedicati.

Tuttavia, sarebbe un errore considerare l'IA come una panacea. Gli stessi strumenti che migliorano la sicurezza introducono nuove superfici di attacco: i modelli di linguaggio possono essere manipolati attraverso tecniche di prompt injection, i sistemi di rilevamento delle anomalie possono essere ingannati con dati avvelenati, le pipeline di aggiornamento automatico dei modelli possono

diventare vettori di compromissione. Una strategia di sicurezza matura deve quindi considerare le soluzioni di IA non solo come strumenti difensivi, ma anche come asset da proteggere.

Il progetto PACY illustra un approccio equilibrato: l'IA viene utilizzata per semplificare e rendere accessibili processi complessi, ma l'utente mantiene il controllo decisionale. Il sistema guida, informa, suggerisce — ma non decide autonomamente. Questo posizionamento è coerente con una visione dell'IA come supporto alle capacità umane piuttosto che come sostituto del giudizio umano, particolarmente appropriato in un dominio dove le conseguenze di una risposta inappropriata possono essere significative.

5.3 Verso un ecosistema digitale più resiliente

La costruzione di un ecosistema digitale resiliente richiede un impegno coordinato su più fronti simultaneamente. Sul piano tecnologico, l'adozione di strumenti avanzati di valutazione dinamica del rischio e di supporto alla risposta agli incidenti deve diventare progressivamente accessibile anche alle organizzazioni più piccole, attraverso soluzioni scalabili e proporzionate alle loro caratteristiche. Sul piano delle competenze, la carenza strutturale di professionisti della cybersecurity — quantificata in milioni di unità a livello globale — richiede investimenti sostenuti in formazione e percorsi di aggiornamento professionale.

Sul piano regolatorio, la NIS2 offre un framework normativo ambizioso, ma la sua efficacia dipenderà dalla qualità del supporto istituzionale offerto alle organizzazioni nella fase di adeguamento. La previsione di obblighi proporzionati e l'accompagnamento delle PMI nel percorso di conformità sono condizioni necessarie perché la direttiva raggiunga gli obiettivi di innalzamento generalizzato della sicurezza digitale che si prefigge.

Il caso italiano, con la sua specificità strutturale legata al peso delle PMI nell'economia nazionale, rende queste considerazioni particolarmente urgenti. Assicurare che anche le organizzazioni più piccole possano accedere a soluzioni di sicurezza efficaci non è solo una questione di compliance normativa, ma una condizione per la competitività e la resilienza dell'intero sistema economico. In questo percorso, l'intelligenza artificiale — opportunamente orientata, limitata nei suoi automatismi e protetta nelle sue vulnerabilità — può svolgere un ruolo determinante come tecnologia abilitante di una sicurezza digitale più diffusa ed equa.

Capitolo 6 – L'Italia dei data center

1. I data center: l'infrastruttura fisica dell'intelligenza artificiale

1.1 Perché l'IA non esiste senza un data center

È ormai un luogo comune affermare che l'intelligenza artificiale stia trasformando ogni settore dell'economia. Lo è molto meno la consapevolezza che quella trasformazione ha un substrato fisico molto preciso: i data center. Ogni query a un modello linguistico generativo, ogni inferenza di un sistema di visione artificiale, ogni ciclo di addestramento di una rete neurale richiede calcolo, memoria, raffreddamento e alimentazione elettrica continua. Queste risorse risiedono in infrastrutture fisiche altamente specializzate — i data center, appunto — che costituiscono, insieme ai chip e alle reti di trasmissione, la triade materiale su cui poggia l'intera economia dell'IA.

Il nesso quantitativo è eloquente: una singola interrogazione a un modello generativo come ChatGPT consuma fino a dieci volte l'energia di una ricerca tradizionale su Google. I modelli di frontiera richiedono per il loro addestramento volumi di dati cresciuti dagli ordini di grandezza dei milioni, tipici degli anni Novanta, a quelli dei miliardi e trilioni di unità registrati nel 2024, con un'accelerazione che riflette la progressiva estensione dell'IA dalla visione artificiale al linguaggio, dalla biologia ai videogiochi. A questa esplosione della domanda computazionale corrisponde un'esplosione speculare dei requisiti energetici e infrastrutturali.

In questo lo studio condotto da The European House of Ambrosetti nel settembre 2025 offre una fotografia sistematica della situazione italiana, proiettandola su scenari al 2035, e delinea le condizioni affinché il Paese possa trasformare la crescita di questi impianti da rischio energetico a opportunità di sviluppo sostenibile e competitività digitale.

1.2 La geografia globale dei data center e il posizionamento italiano

Nel 2024 sono censiti 10.332 data center a livello globale, distribuiti in 168 paesi. La concentrazione geografica è marcata: gli Stati Uniti ospitano da soli 5.426 impianti, seguiti dall'Unione Europea con 2.254, seconda potenza mondiale per capacità installata. In questo

contesto, l'Italia si colloca al 13° posto mondiale con 168 data center attivi, per una superficie complessiva superiore a 333.000 m² e una potenza nominale totale di 513 MW, in crescita del 17% rispetto all'anno precedente.

La distribuzione geografica interna è fortemente polarizzata: oltre il 60% della capacità nazionale (318 MW) è concentrata in Lombardia. Il polo di Milano, con 238 MW, rappresenta il 46% del totale nazionale e si posiziona al primo posto tra i mercati emergenti europei, superando Madrid (172 MW) e oltre il doppio di Zurigo (110 MW). Questo dato acquista rilevanza strategica nel contesto del progressivo rallentamento degli hub storici europei — il cosiddetto cluster FLAPD, ovvero Francoforte (867 MW), Londra (1.065 MW), Amsterdam (544 MW), Parigi (400 MW) e Dublino (296 MW) — che pur detenendo circa l'80% della domanda continentale mostra segnali evidenti di saturazione e contrazione delle nuove installazioni.

Per l'Italia e in particolare per Milano si è aperta una finestra di opportunità che gli investitori internazionali hanno già iniziato a cogliere. Le richieste di connessione alla rete ad alta tensione di Terna per la realizzazione di nuovi data center sono passate da 0,1 GW nel 2019 a oltre 55 GW nei primi otto mesi del 2025, per un totale di 342 domande, di cui oltre l'80% localizzate nel Nord Italia e il 57% in Lombardia. Una crescita senza precedenti che non è solo un indicatore di interesse, ma un segnale della pressione strutturale che si sta formando sui sistemi energetici e infrastrutturali del Paese.

2. La sfida energetica: quadruplicare i consumi senza destabilizzare il sistema

2.1 Le proiezioni al 2035: uno scenario di trasformazione strutturale

Il dato più impattante che emerge dall'analisi riguarda la traiettoria dei consumi energetici. A livello globale, le stime IEA e BloombergNEF indicano che il consumo elettrico dei data center potrebbe passare da 371 TWh nel 2024 a quasi 1.600 TWh nel 2035, quadruplicando in poco più di un decennio e raggiungendo circa il 4% dei consumi mondiali di elettricità (rispetto all'attuale 1%). L'80% di questa crescita sarà generata da tre aree: Stati Uniti (+240 TWh, +130%), Cina (+175 TWh, +170%) ed Europa.

Per l'Italia, le proiezioni sono ancora più pronunciate in termini relativi. Secondo gli scenari elaborati da TEHA, la potenza installata dei data center nazionali potrebbe crescere dagli attuali 513 MW a 2.300 MW nello scenario tendenziale al 2035, e fino a 4.573 MW in uno scenario di pieno sviluppo (full potential). L'incidenza sui consumi elettrici nazionali salirebbe dall'1,9% del 2024 al 7,4% nello scenario tendenziale, fino al 12,7% nello scenario full potential. Per dare una misura della portata di questo cambiamento: in Irlanda, paese in cui la crescita dei data center non è stata adeguatamente pianificata, questi impianti rappresentano già il 21% del consumo elettrico nazionale, equivalente all'intero settore residenziale del Paese. In Virginia, la concentrazione di data center ha portato a un aumento del 65% del consumo idrico dall'anno 2019, con effetti sull'intero equilibrio delle risorse locali.

Gli investimenti necessari a sostenere questa espansione sono nell'ordine dei miliardi: tra 23 e 35 miliardi di euro nello scenario tendenziale, fino a circa 69 miliardi di euro nello scenario full potential. Una cifra che conferma come lo sviluppo dei data center non sia più una questione meramente tecnologica, ma una scelta industriale e finanziaria di sistema.

Tabella 1 — Principali indicatori del settore data center in Italia: stato attuale e scenari al 2035

Indicatore	Valore 2024	Scenario tendenziale 2035	Scenario full potential
Potenza installata (MW IT)	513 MW	2.300 MW	4.573 MW
Incidenza su consumi elettrici naz.	1,9%	7,4%	12,7%
Data center attivi in Italia	168	—	—
Richieste connessione a Terna	55 GW (2025)	—	—
Contributo alla crescita PIL	—	6,4% crescita/anno	15,6% crescita/anno
Occupazione abilitata	—	>77.000 addetti	>150.000 addetti
Investimenti necessari (mld €)	—	23-35	~69
CO_2 evitata (Mt/anno)	—	—	5,7 Mt

Fonte: elaborazione TEHA Group su dati Politecnico di Milano, Terna e IEA, 2025. Scenario tendenziale calcolato sulla base di progetti in costruzione o in fase avanzata. Scenario full potential include l'applicazione integrata di tutte le leve di efficienza identificate.

2.2 Il problema del profilo di consumo baseload

I data center non si limitano ad aggiungere volumi di consumo al sistema elettrico: ne modificano strutturalmente la natura. A differenza della gran parte degli usi elettrici tradizionali — che presentano variazioni significative tra giorno e notte, estate e inverno — i data center richiedono un'alimentazione continua, stabile e priva di interruzioni, con un profilo di consumo costante nelle 24 ore per 365 giorni l'anno. Questo profilo baseload crea tensioni specifiche con la caratteristica intrinsecamente intermittente delle fonti energetiche rinnovabili, che costituiscono un pilastro irrinunciabile della decarbonizzazione del sistema elettrico.

La soluzione non può essere la rinuncia alle rinnovabili, ma la loro integrazione con fonti flessibili e affidabili. In Italia, le centrali termoelettriche a ciclo combinato emergono come risorsa strategica

di bilanciamento: nel Paese sono operative 56 unità, che utilizzano solo il 30% della capacità complessiva disponibile, offrendo un margine significativo per gestire la crescita futura della domanda digitale. Sono stati inoltre recentemente realizzati tre nuovi impianti a ciclo combinato e ne sono previsti altri tre, per una potenza totale aggiuntiva di quasi 5 GW. A livello internazionale, i grandi operatori digitali si stanno muovendo verso accordi di lungo termine con la generazione nucleare: Microsoft ha stipulato un contratto ventennale per 800 MW con una centrale riattivata in Pennsylvania, mentre Google è impegnata nello sviluppo di reattori modulari di piccola taglia (SMR) in partnership con Kairos Power, con avvio del primo impianto previsto entro il 2030.

Sul fronte dell'efficienza energetica, un indicatore chiave è il Power Usage Effectiveness (PUE): il rapporto tra l'energia totale assorbita dal data center e quella effettivamente utilizzata dall'hardware IT. Il PUE medio mondiale varia da 1,67 per gli impianti sotto 1 MW a 1,44 per quelli oltre 20 MW, confermando che la scala è un fattore determinante di efficienza e che l'aggregazione degli impianti in strutture più grandi e integrate rappresenta una strategia razionale tanto sul piano economico quanto su quello ambientale. Il quadro normativo europeo, con il Regolamento Delegato (UE) 2024/1364 che introduce 24 indicatori di performance — il 75% dei quali direttamente legati all'efficienza energetica — spinge in questa stessa direzione.

3. I data center come opportunità: valore economico, occupazione e circolarità

3.1 La Data Economy italiana e il moltiplicatore dei data center

L'analisi inquadra lo sviluppo dei data center all'interno di un fenomeno più ampio: la crescita della Data Economy italiana, definita come l'insieme delle attività che creano valore lungo il ciclo di vita dei dati. Nel 2024, la Data Economy italiana vale circa 60,6 miliardi di euro, pari al 2,8% del PIL nazionale, collocando il Paese al quarto posto nell'Unione Europea, dietro a Regno Unito (170,6 miliardi), Germania (164,5 miliardi) e Francia (87,2 miliardi). Il potenziale di crescita è considerevole: se l'Italia raggiungesse il peso sul PIL dei migliori performer europei (circa il 7,9% del PIL registrato da paesi come Estonia, Finlandia e Paesi Bassi), il valore della Data Economy potrebbe arrivare a 207 miliardi di euro entro il 2030, rispetto ai 95,7 miliardi attesi nello scenario tendenziale.

I driver di questa crescita sono strutturali: dal 2005 al 2024 la quota di popolazione mondiale connessa a Internet è aumentata di oltre 50 punti percentuali, raggiungendo il 67,6%, con oltre 4 miliardi di utenti addizionali. In Italia il traffico dati su rete fissa ha registrato un incremento di 2,7 volte tra il 2019 e il 2024 (da 0,23 a 0,86 GB per utente), con previsioni di crescita media annua del 14% fino al 2040. Il mercato dei servizi cloud ha segnato una crescita del 24% tra 2023 e 2024, superiore persino al picco pandemico del 2020 (+20%), con proiezioni di crescita annua del 10,3% fino al 2040. Il settore IoT, con circa 2,6 dispositivi connessi per abitante e un valore di mercato di 9,7 miliardi di euro, completa il quadro di una domanda digitale che spinge strutturalmente verso una capacità computazionale e di archiviazione crescente.

In questo contesto, i data center non sono semplici consumatori passivi di risorse: sono abilitatori di valore economico. TEHA stima che ogni punto percentuale di crescita del PIL italiano sarà attribuibile, nello scenario full potential, per 0,16 punti percentuali all'espansione del settore dei data center. Il contributo alla crescita annua del PIL potrebbe variare dal 6,4% nello scenario tendenziale al 15,6% nello scenario di pieno sviluppo. L'occupazione diretta, indiretta e indotta associata potrebbe raggiungere oltre 77.000 addetti nello scenario tendenziale e oltre 150.000 in quello full potential.

3.2 Il modello circolare: dalla dipendenza energetica alla produzione di valore

Il contributo più originale dell'analisi riguarda la possibilità di trasformare i data center da infrastrutture puramente energivore a protagonisti attivi della transizione ecologica, attraverso un modello di economia circolare che valorizza le esternalità positive di questi impianti.

La prima e più significativa di queste esternalità è il calore di scarto. I server generano calore continuo che oggi viene in larga parte disperso nell'atmosfera tramite sistemi di raffreddamento a elevato consumo energetico. TEHA stima che, in uno scenario di sviluppo full potential, il calore recuperabile dai data center localizzati in prossimità di reti di teleriscaldamento esistenti o pianificate possa raggiungere i 9,5 TWh annui, equivalenti al fabbisogno termico di 800.000 famiglie italiane — di cui oltre 530.000 nella sola area metropolitana di Milano. Il beneficio climatico sarebbe di due milioni di tonnellate di CO_2 risparmiate all'anno, corrispondenti al 5% delle emissioni del settore residenziale italiano, un valore paragonabile alla riduzione di emissioni

dell'intero decennio precedente nel settore. Esempi concreti sono già in corso: il data center Qarnot nella centrale Lamarmora di Brescia, inaugurato nel 2025 da A2A, e il progetto Avalon 3 a Milano che dal 2026 consentirà di recuperare oltre 15 GWh termici all'anno.

La seconda leva riguarda il consumo di suolo. TEHA ha mappato 3,7 milioni di m² di aree industriali dismesse (brownfield) idonee alla localizzazione di data center, con oltre 180 siti già individuati, sufficienti a ospitare impianti per oltre 3,5 GW di potenza IT. Il 16% di questi siti dispone già di un allaccio in media o alta tensione, riducendo tempi e costi di connessione alla rete. L'utilizzo di aree brownfield permetterebbe di preservare una superficie di suolo pari a 84 campi da calcio — o, detto altrimenti, alla superficie occupata da 50.000 alberi — contribuendo alla rigenerazione urbana anziché al consumo di territorio vergine.

Una terza dimensione riguarda l'approvvigionamento energetico rinnovabile tramite Power Purchase Agreements (PPA): contratti di lungo termine che garantiscono forniture stabili e tracciabili e incentivano nuovi investimenti in capacità verde. In uno scenario full potential fino al 74% del fabbisogno energetico dei data center italiani potrebbe essere coperto da rinnovabili tramite PPA, per un totale di oltre 30,9 TWh annui e una riduzione stimata di 3,7 milioni di tonnellate di CO_2 all'anno. Infine, la gestione dei RAEE (Rifiuti da Apparecchiature Elettriche ed Elettroniche) generati dai data center — stimati in oltre 147.000 tonnellate annue, di cui circa 74.000 riciclabili — potrebbe attivare una filiera nazionale di trattamento con un valore economico di 133 milioni di euro l'anno.

Nel complesso, l'applicazione integrata di tutte queste leve di efficienza permetterebbe, secondo l'analisi condotta, di evitare 5,7 milioni di tonnellate di CO_2 annue — equivalenti alle emissioni di 1,7 milioni di cittadini italiani — e di generare un beneficio economico totale di circa 1,7 miliardi di euro, inclusi il valore del carbonio evitato (956 milioni), i risparmi nel sistema ETS (619 milioni) e i proventi dal riciclo dei RAEE (133 milioni).

4. Governance, pianificazione e ruolo istituzionale

4.1 La necessità di un approccio strategico nazionale

L'esperienza internazionale insegna che la crescita dei data center non pianificata produce conseguenze negative difficilmente reversibili. Il caso irlandese è emblematico: senza una governance coordinata, i data center hanno raggiunto il 21% del consumo elettrico nazionale, saturando le reti e creando tensioni strutturali sul sistema energetico dell'isola. In Virginia, la concentrazione di impianti ha innescato una crisi idrica con un aumento del 65% del consumo d'acqua, mettendo sotto pressione le risorse locali e alimentando opposizioni comunitarie.

In Italia, la consapevolezza di questa sfida ha iniziato a tradursi in iniziative istituzionali concrete. Nel 2024 sono state presentate in Parlamento numerose proposte di legge per semplificare le autorizzazioni, potenziare le infrastrutture elettriche e riconoscere i data center come opere strategiche nazionali. Nel luglio 2025 il Ministero delle Imprese e del Made in Italy ha avviato una consultazione pubblica per definire una strategia nazionale di attrazione degli investimenti esteri nel settore, con l'obiettivo di posizionare l'Italia come hub competitivo per le infrastrutture digitali avanzate. Si inserisce nello stesso filone il regime di incentivazione e semplificazione amministrativa previsto per le cosiddette Zone Economiche Speciali Digitali, in via di definizione normativa.

Questi segnali istituzionali vanno nella giusta direzione, ma la sfida richiede un coordinamento tra più livelli: quello energetico (mix di generazione, bilanciamento della rete, contratti di lungo termine per le rinnovabili), quello urbanistico (individuazione delle aree brownfield, integrazione con le reti di teleriscaldamento), quello finanziario (attrazione degli investimenti internazionali, sostegno alle filiere locali), e quello regolatorio (adeguamento dei tempi autorizzativi, recepimento della normativa europea sull'efficienza dei data center). Lo sviluppo sostenibile del settore richiede quindi una pianificazione strategica integrata, non una somma di interventi settoriali.

4.2 Il nesso con la geopolitica dell'IA

Lo sviluppo dei data center italiani non è una questione meramente nazionale: si inserisce in un contesto geopolitico in cui il controllo delle infrastrutture di calcolo rappresenta una delle

dimensioni fondamentali della competizione per la leadership nell'intelligenza artificiale. Come si è già discusso in questo documento a proposito della geopolitica dell'IA e della mappa delle terre rare, la catena del valore dell'IA comprende strati fisici distinti — dalle materie prime critiche per i chip, ai semiconduttori, fino alle infrastrutture fisiche di calcolo — e la posizione di ciascun attore in questa catena determina la propria capacità di sviluppare, dispiegare e governare sistemi di IA avanzati.

In questo quadro, l'Italia e l'Europa si trovano in una posizione di relativa debolezza strutturale rispetto agli Stati Uniti e alla Cina: assenza di produttori di chip di frontiera, dipendenza da fornitori extra-europei per le terre rare, e — fino a poco tempo fa — anche marginalità nel mercato dei data center di grandi dimensioni. La finestra di opportunità che si è aperta con la saturazione degli hub FLAPD rappresenta quindi non solo un'opportunità economica per il Paese, ma un tassello della più ampia strategia europea di riduzione delle dipendenze digitali, espressa con il concetto di sovranità digitale e perseguita attraverso iniziative come l'AI Act, il Digital Markets Act e — appunto — l'attrazione di investimenti in infrastrutture di calcolo.

La tesi del NVIDIA CEO Jensen Huang sull' "intelligenza artificiale sovrana" — per cui ogni nazione dovrebbe disporre di proprie infrastrutture di calcolo per non essere dipendente da operatori stranieri nelle funzioni cognitive più critiche — trova in questo contesto una concretizzazione molto pratica: i data center pubblici e privati che vengono costruiti oggi in Italia e in Europa sono, insieme alle normative che ne governano la localizzazione, il funzionamento e i flussi di dati, una delle forme concrete attraverso cui la sovranità digitale prende corpo.

4.3 Le relazioni con le comunità

La realizzazione di grandi impianti di produzione di energia o di gestione della stessa è sempre stato un tema che ha frammentato l'opinione pubblica, fino ad influenzare movimenti sociali e politici. Nel 2025 un giornalista, Matteo Wong, ha visitato Colossus, il data center a quell'epoca in costruzione da parte di Elon Musk per il futuro sviluppo di Grok (soluzione di AI dell'azienda da lui fondata, xAI). Lo descrisse come un hangar grande più di dieci campi di calcio, che necessita di una elettricità doppia rispetto all'intera città di Seattle. Ovviamente Musk non è il solo ad investire in questa direzione: Microsoft ha acquisito una centrale nucleare dismessa in USA (Three Mile

Island, nota anche per il peggior incidente nucleare nella storia statunitense), mentre Amazon sta puntando ad installare dei reattori nucleari su mezzi pensanti in movimento per garantire la produzione di energia necessaria ad alimentare l'AI. La corsa all'energia, per certi versi non pulita, rappresenta una delle differenze strategiche tra USA e Cina: quest'ultima sta investendo pesantemente in nuova capacità solare ed eolica, anziché optare per quella nucleare o sui combustibili fossili.

Ma al di là dell'aspetto strategico, questi investimenti spostano enormi quantitativi di denaro e di conseguenza anche interessi puramente territoriali. Mentre le istituzioni politiche locali vedono con ardore l'intercettazione di questi enormi capitali, tra le comunità sorge un certo scetticismo: ad aprile 2026 il Maine è diventato il primo Stato ad approvare una moratoria sulla costituzione dei data center; il 70% dei residenti del Wisconsin è convinto che i costi di costituzione di un centro superino di gran lunga i benefici; molte persone in alcuni stati statunitensi raccontano di aver scoperto dell'esistenza di un progetto grazie a una richiesta di modifica della destinazione del suolo presentata da un'azienda di cui nessuno aveva mai sentito parlare, infine spesso nelle sale comunali, i progetti relativi ad accordi con i privati per la realizzazione di queste infrastrutture sono intitolati con nomi in codice, per evitare di creare scalpore e attirare l'opposizione mediatica. Da qui nascono movimenti popolari e in parte politici per sostenere i diritti dei cittadini alla contrarietà di queste costruzioni. A ciò si aggiunga che internet e l'AI rappresentano tecnologie nella concezione popolare "astratte", il cui funzionamento nella percezione dell'utente medio è nel "cloud", una nuvola nell'etere, mentre i data center sono luoghi specifici dove le persone possono riunirsi e ritrovarsi a combattere per gli stessi ideali. Accadrà lo stesso in Italia?

5. Considerazioni conclusive

Il Position Paper di TEHA Group restituisce un'immagine dell'Italia a un bivio: la crescita dei data center è un fenomeno già in atto, accelerato dalla corsa globale all'IA, che il Paese non può né fermare né ignorare. La questione non è se i data center cresceranno, ma come cresceranno e chi ne catturerà il valore.

Lo scenario tendenziale porterebbe la potenza installata a 2,3 GW entro il 2035, con un'incidenza del 7,4% sui consumi elettrici nazionali e un contributo potenziale del 6,4% alla crescita annua del

PIL. Lo scenario full potential — condizionato all'adozione coordinata di leve di efficienza, pianificazione strategica e investimenti infrastrutturali — porterebbe questi parametri rispettivamente a 4,6 GW, 12,7% dei consumi e 15,6% del contributo alla crescita del PIL, con oltre 150.000 occupati e 5,7 milioni di tonnellate di CO_2 evitate l'anno.

La distinzione tra i due scenari non è determinata dalla domanda di mercato — quella cresce in entrambi i casi — ma dalla qualità della risposta istituzionale, industriale e infrastrutturale. Un paese che pianifica bene lo sviluppo dei data center — individuando le aree brownfield, integrando gli impianti con le reti di teleriscaldamento, garantendo la copertura rinnovabile tramite PPA, semplificando le autorizzazioni senza rinunciare ai requisiti di efficienza — può trasformare un'infrastruttura energivora in un hub multifunzionale di energia e innovazione.

Il legame con l'intelligenza artificiale è diretto e non mediabile: senza data center di qualità, scalabili e alimentati in modo affidabile, non esiste capacità di sviluppare o dispiegare sistemi di IA avanzati sul proprio territorio. L'infrastruttura di calcolo è, in questo senso, la precondizione fisica di ogni ambizione di sovranità digitale. E il momento per costruirla — o lasciare che altri la costruiscano per noi — è adesso.

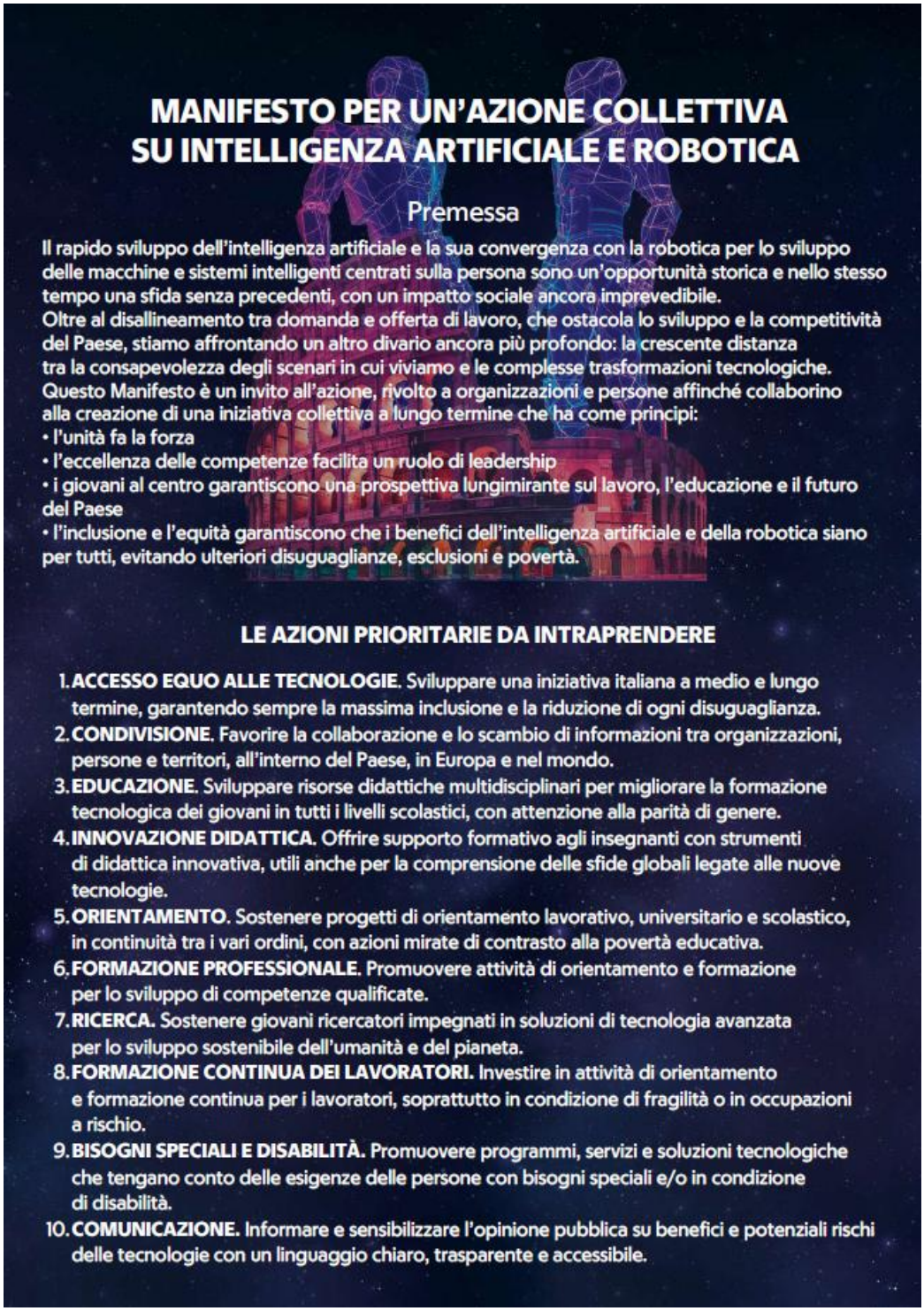
Manifesto dell'AI e della Robotica

Fin dal 2024, l'Associazione AIdAM si è impegnata sul tema dell'intelligenza artificiale. Il primo passo è stato quello di creare un Osservatorio AI, all'interno dell'Ufficio Studi, per mappare e monitorare tutti i casi applicativi in ambito automazione e robotica che prevedevano testo o impiego su larga scala dell'AI. Questo repository è a disposizione dei soci AIdAM per approfondire ciò che sta accadendo nel mondo, in particolare nel nostro settore industriale.

Subito dopo, AIdAM è entrata in contatto con Fondazione Mondo Digitale e ha aderito all'iniziativa di redigere e siglare un Manifesto per un'azione collettiva sull'intelligenza artificiale e sulla robotica. Si tratta di un progetto di lungo periodo per un'alleanza comune e strategica volta a far collaborare diversi attori nella direzione di un rispetto dell'etica e dello sviluppo sostenibile di una tecnologia che sta già cambiando le nostre viste.

AIdAM ha siglato il Manifesto, insieme ad aziende come Microsoft Italia, SAP Italia, Istituto Italiano di Tecnologia (IIT), Avanade Italy, ING Italia, Johnson & Johnson Innovative Medicine Italia e numerose università italiane. A questo link l'elenco dei soggetti sottoscrittori: https://www.mondodigitale.org/formazione/risorse-educative/manifesto-unazione-collettiva-su-intelligenza-artificiale-e-robotica

Qui di seguito si riporta il Manifesto.



MANIFESTO PER UN'AZIONE COLLETTIVA SU INTELLIGENZA ARTIFICIALE E ROBOTICA

Premessa

Il rapido sviluppo dell'intelligenza artificiale e la sua convergenza con la robotica per lo sviluppo delle macchine e sistemi intelligenti centrati sulla persona sono un'opportunità storica e nello stesso tempo una sfida senza precedenti, con un impatto sociale ancora imprevedibile.
Oltre al disallineamento tra domanda e offerta di lavoro, che ostacola lo sviluppo e la competitività del Paese, stiamo affrontando un altro divario ancora più profondo: la crescente distanza tra la consapevolezza degli scenari in cui viviamo e le complesse trasformazioni tecnologiche.
Questo Manifesto è un invito all'azione, rivolto a organizzazioni e persone affinché collaborino alla creazione di una iniziativa collettiva a lungo termine che ha come principi:

- l'unità fa la forza
- l'eccellenza delle competenze facilita un ruolo di leadership
- i giovani al centro garantiscono una prospettiva lungimirante sul lavoro, l'educazione e il futuro del Paese
- l'inclusione e l'equità garantiscono che i benefici dell'intelligenza artificiale e della robotica siano per tutti, evitando ulteriori disuguaglianze, esclusioni e povertà.

LE AZIONI PRIORITARIE DA INTRAPRENDERE

1. **ACCESSO EQUO ALLE TECNOLOGIE**. Sviluppare una iniziativa italiana a medio e lungo termine, garantendo sempre la massima inclusione e la riduzione di ogni disuguaglianza.
2. **CONDIVISIONE**. Favorire la collaborazione e lo scambio di informazioni tra organizzazioni, persone e territori, all'interno del Paese, in Europa e nel mondo.
3. **EDUCAZIONE**. Sviluppare risorse didattiche multidisciplinari per migliorare la formazione tecnologica dei giovani in tutti i livelli scolastici, con attenzione alla parità di genere.
4. **INNOVAZIONE DIDATTICA**. Offrire supporto formativo agli insegnanti con strumenti di didattica innovativa, utili anche per la comprensione delle sfide globali legate alle nuove tecnologie.
5. **ORIENTAMENTO**. Sostenere progetti di orientamento lavorativo, universitario e scolastico, in continuità tra i vari ordini, con azioni mirate di contrasto alla povertà educativa.
6. **FORMAZIONE PROFESSIONALE**. Promuovere attività di orientamento e formazione per lo sviluppo di competenze qualificate.
7. **RICERCA**. Sostenere giovani ricercatori impegnati in soluzioni di tecnologia avanzata per lo sviluppo sostenibile dell'umanità e del pianeta.
8. **FORMAZIONE CONTINUA DEI LAVORATORI**. Investire in attività di orientamento e formazione continua per i lavoratori, soprattutto in condizione di fragilità o in occupazioni a rischio.
9. **BISOGNI SPECIALI E DISABILITÀ**. Promuovere programmi, servizi e soluzioni tecnologiche che tengano conto delle esigenze delle persone con bisogni speciali e/o in condizione di disabilità.
10. **COMUNICAZIONE**. Informare e sensibilizzare l'opinione pubblica su benefici e potenziali rischi delle tecnologie con un linguaggio chiaro, trasparente e accessibile.

Fonti utilizzate

Questa pubblicazione realizzata dall'Ufficio Studi AIdAM ha utilizzato le seguenti fonti di analisi come base dati.

Rivista di Politica economica di Confindustria – Ufficio Studi Confindustria (n.2 2024)

L'intelligenza artificiale per il sistema Italia, Confindustria - Report 2025

L'Italia dei data center – The European House of Ambrosetti e A2A (settembre 2025)

Osservatorio Artificial Intelligence, Politecnico di Milano — Ricerca 2025 (febbraio 2026)

ISTAT — Rapporto Annuale 2026 (maggio 2026) e Imprese e ICT 2025 (dicembre 2025)

Osservatorio Innovazione Digitale nelle PMI, Politecnico di Milano — Ricerca 2025-2026 (maggio 2026)

Osservatorio Innovative Robotics, Politecnico di Milano — Ricerca 2026 (giugno 2026)

Osservatorio Contract Logistics "Gino Marchet", Politecnico di Milano — Ricerca 2026 (febbraio 2026)

i-LOG — Osservatorio Radar IA, Università Cattaneo-LIUC (2026)

UCIMA — Preconsuntivi settore macchine packaging 2025 (Centro Studi MECS, gennaio 2026)

Federalimentare / Confagricoltura — Rapporto Agrifood Tech Italia 2026 (Camera dei Deputati, aprile 2026)

AlixPartners — Presentazione Food Summit 2026 (maggio 2026)

McKinsey & Company — The Future of the Agrifood Industry (2025)

ZS Associates — AI in Pharma R&D: Success Rate Analysis (2025-2026)

Antares Vision Group — Metpack 2026, comunicati tecnici (maggio 2026)

Siemens — SPS Italia 2026, comunicati tecnici (maggio 2026)

U.S. Geological Survey – Mineral Commodity Summaries 2025

IEA – Energy and AI 2025

IEA – Global Critical Minerals Outlook 2025

Parlamento europeo – Risoluzione sulle restrizioni cinesi all'export di terre rare, ottobre 2025

TRADIUM – Market Analysis 2025; World Bank Mining Forum 2024

Rivista Internazionale n.1668 – 5 giugno 2026

ALLEGATI – Case study delle aziende AIdAM

Case History 1 – Awentia Srl

Vedere dal primo pezzo. Physical AI zero-shot: portare una percezione simile a quella umana nell'ispezione, nella robotica e nell'automazione industriale, senza dataset e senza training.

1. Lunedì, ore 6

Il cliente invia una nuova variante di prodotto. Un nuovo colore, una texture diversa, un fornitore di materia prima che cambia. La linea è pronta a ripartire. Il sistema di visione no: non ha mai visto quel prodotto, e per lui è come essere cieco.

Da qui comincia un percorso che chiunque abbia portato l'intelligenza artificiale in fabbrica conosce bene. Servono immagini, migliaia, etichettate a mano difetto per difetto. Poi l'addestramento, poi la validazione. Settimane in cui la linea aspetta, oppure produce senza un controllo qualità automatico. E quando il prodotto cambia di nuovo, il ciclo ricomincia.

Questo contributo racconta come Awentia ha affrontato il problema alla radice, partendo da una domanda semplice: **e se il sistema di visione non avesse bisogno di un dataset?**

2. Il mercato e il nodo della produzione

La visione artificiale è entrata in una fase di crescita strutturale: più macchine automatiche, più robot, più controlli in linea, e un'intelligenza artificiale che ogni anno ne allarga il campo d'applicazione. Eppure questa crescita ha un tappo.

<10%

dei progetti pilota di intelligenza artificiale arriva alla produzione su larga scala

International Institute for Analytics, 2019[1]

La crescita c'è. Il mercato mondiale della machine vision cresce a ritmo sostenuto e continuerà a farlo per tutto il decennio,[2] trainato da un parco di robot industriali che in dieci anni è più che raddoppiato.[3] Ogni nuova macchina, ogni nuova cella, ogni linea da rinnovare è una macchina che ha bisogno di vedere.

Ma si ferma al pilota. Meno di un progetto di AI su dieci arriva alla produzione su larga scala. Non perché la tecnologia non funzioni: in laboratorio le prove funzionano. Si fermano quando incontrano la linea reale, con i cambi di prodotto, i materiali che variano, i difetti che nel dataset non ci sono. Ogni nuova applicazione riparte da zero, e il costo di ripartire finisce per superare il valore che l'AI dovrebbe portare.

Per accelerare serve un tassello diverso. Al mercato non servono più progetti pilota, ma qualcosa che li porti in produzione: un componente di percezione che si installa come un sensore, si configura descrivendo che cosa cercare e non va riaddestrato a ogni cambio. È il ruolo per cui è nato **AVT Physical AI Core©**: fare il lavoro sui dati una volta, a monte, perché costruttori e integratori possano portare la visione in macchina come una funzione di prodotto. E alzare, finalmente, quel 10%.

---

[1] International Institute for Analytics (IIA), 2019. https://iianalytics.com/

[2] MarketsandMarkets, «Machine Vision Market – Global Forecast to 2030», maggio 2025: da 15,8 miliardi di dollari nel 2025 a 23,6 miliardi nel 2030 (+8,3% l'anno). https://www.marketsandmarkets.com/Market-Reports/machine-vision-market-431.html

[3] IFR – International Federation of Robotics, «World Robotics 2025», 25 settembre 2025: 542.000 robot industriali installati nel 2024, più del doppio di dieci anni prima. https://ifr.org/ifr-press-releases/news/global-robot-demand-in-factories-doubles-over-10-years

> *Il problema non è far funzionare l'AI in un progetto pilota. È farla funzionare il lunedì dopo, quando il prodotto cambia.*

3. Il collo di bottiglia non è la telecamera

Negli ultimi dieci anni il deep learning ha reso possibili ispezioni che la visione artificiale tradizionale, basata su regole e soglie, non riusciva ad affrontare: superfici naturali, difetti dalla forma imprevedibile, prodotti con grande variabilità estetica. Ma ha spostato il costo dal sensore al dato.

Un modello supervisionato convenzionale richiede, per ogni prodotto e per ogni tipo di difetto, una raccolta sistematica di immagini, un'etichettatura manuale accurata, un ciclo di addestramento e una validazione. Servono competenze di data science che raramente sono presenti in un'azienda manifatturiera, e il risultato è rigido: basta cambiare formato, fornitore o anche solo l'illuminazione del reparto perché le prestazioni degradino. A quel punto si ferma la linea, si raccolgono nuovi dati e si riaddestra.



Figura 1. Dal ciclo "raccogli, etichetta, addestra" al paradigma "descrivi, verifica, installa".

Va detto con onestà: l'approccio tradizionale funziona, a due condizioni. La prima è che ogni caratteristica da rilevare sia presente nel dataset in modo **bilanciato**. La seconda è che il dataset sia **rappresentativo** della variabilità reale dell'applicazione finale. Nessuna delle due è semplice da soddisfare. Su una linea ben gestita i difetti sono, per definizione, rari: raccoglierne abbastanza esempi, di ogni tipo, richiede mesi. E la variabilità reale cambia nel tempo, con lotti, stagioni e materie prime.

Il risultato è quello visto sopra: **i progetti si fermano al pilota.** Per un costruttore di macchine questo significa che ogni installazione diventa un progetto di intelligenza artificiale su misura; per un responsabile di stabilimento, che il ritorno dell'investimento in visione si assottiglia a ogni cambio di produzione.

Il tema è particolarmente sentito nella manifattura italiana, fatta di lotti piccoli, alta varietà di prodotto e materiali naturali come pelle, legno, pietra e tessuti, dove la variabilità non è un'eccezione da gestire ma la natura stessa del prodotto. È il contesto in cui un modello addestrato su un dataset fisso fa più fatica, e in cui un approccio diverso può fare la differenza.

> *Il dataset è la garanzia che l'AI funzioni. E quando i dati adeguati non esistono, che sulla linea reale è la situazione normale, non c'è garanzia.*

4. Dal training alla descrizione: lo zero-shot

Una risposta arriva dai **modelli fondazionali di visione** e dai **Vision-Language Model**: modelli generalisti, addestrati su insiemi molto ampi e diversificati di immagini e testo. Questi modelli sanno già che cos'è un graffio, un foro, una crepa o un biscotto rotto. Non hanno bisogno di imparare il prodotto del cliente: hanno bisogno di sapere **che cosa cercare**.

È il principio dell'apprendimento **zero-shot**: riconoscere una categoria senza averne mai visto esempi etichettati, a partire da una descrizione. In questo approccio l'ispezione è definita da un **prompt**, che può essere una breve descrizione testuale ("trova i graffi su questa pelle") oppure un riferimento visivo del difetto. Dal primo pezzo in linea il sistema identifica, segmenta e classifica ciò che è stato richiesto.

Il cambio di paradigma è tutto qui: si passa dall'**addestrare su dati** al **descrivere un obiettivo**. E quando il prodotto cambia non si riaddestra nulla: si cambia il prompt.

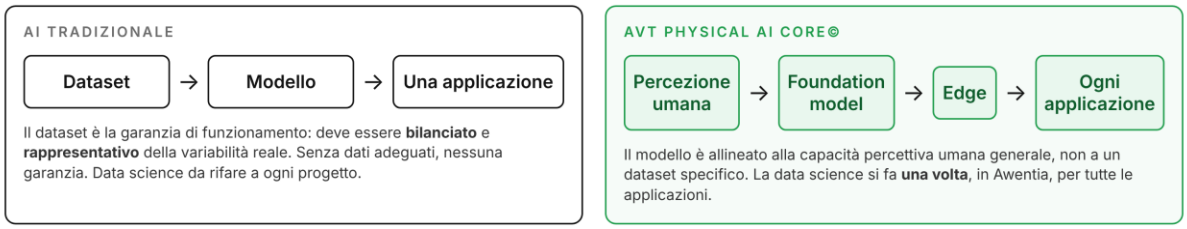


Figura 2. Due logiche a confronto: un modello legato a un dataset e a una sola applicazione, oppure un modello allineato alla percezione umana e riutilizzabile ovunque.

Un ispettore qualità esperto, davanti a un prodotto che non ha mai visto, sa comunque riconoscere un graffio, una macchia o una deformazione. Non ha bisogno di mille esempi di quel difetto su quel prodotto: porta con sé una capacità percettiva generale e la applica al caso specifico, guidato da un'indicazione su che cosa conta.

Un modello zero-shot lavora allo stesso modo. Anziché allinearlo a un singolo dataset, lo si allinea alla **capacità percettiva umana generale** e lo si porta così com'è, con tutta la sua capacità di generalizzazione, direttamente sul dispositivo edge accanto alla linea. Il lavoro di data science si fa **una volta, a monte, per tutte le applicazioni**, e non va ripetuto a ogni nuovo progetto.

5. Come funziona, in pratica

Nell'implementazione sviluppata da Awentia, AVT Physical AI Core©, l'architettura è volutamente semplice da integrare in una linea esistente o in una macchina nuova.



Figura 3. Architettura di AVT Physical AI Core©: dall'immagine e dal prompt alla decisione, interamente on-premise.

- **Input.** Le immagini arrivano da telecamere industriali standard. Insieme all'immagine, il modello riceve il prompt che definisce l'ispezione.
- **Elaborazione edge.** Il modello fondazionale di visione gira su un dispositivo edge a bordo linea o a bordo macchina. L'ispezione avviene in tempo reale e interamente on-premise: nessuna immagine lascia lo stabilimento, nessuna dipendenza dal cloud, nessuna latenza di rete.
- **Output.** Il risultato è una decisione chiara, OK o NOK, accompagnata da una **maschera di segmentazione** che indica dove si trova il difetto e quanto è esteso, con la relativa classe e severità. Un piccolo segno superficiale e un taglio profondo non portano alla stessa decisione.

Per la configurazione sono disponibili due modalità, pensate per persone diverse:

- l'**interfaccia standard**, per il vision engineer che vuole il pieno controllo di parametri, soglie e tolleranze;
- l'**interfaccia agentica**, un assistente AI con cui l'operatore descrive il difetto in linguaggio naturale e l'agente configura l'ispezione. Si può chiedere, ad esempio, di essere più tolleranti sulle piccole variazioni di colore di un tessuto.

> *L'ispezione parte da una descrizione, non da un dataset: "vorrei trovare i graffi su questo pezzo di pelle". Il resto (ottiche, luce, integrazione, verifica sui pezzi reali) resta il lavoro di sempre, ed è quello che fa la differenza.*

6. Dalla visione all'azione: Physical AI per robotica e automazione

Con **Physical AI** si indica l'intelligenza artificiale che percepisce il mondo fisico e agisce in esso: robot, macchine automatiche, veicoli, sistemi di movimentazione. In tutti questi sistemi la percezione è il primo anello della catena e, spesso, il più fragile. Un robot può essere estremamente preciso nei movimenti, ma se non riconosce l'oggetto che ha davanti, o lo riconosce solo nelle condizioni in cui è stato addestrato, la sua flessibilità resta sulla carta.

È qui che la percezione di tipo umano diventa un abilitatore. Lo stesso principio usato per il controllo qualità vale per guidare un'azione: si descrive che cosa riconoscere e il sistema restituisce non solo una classe, ma la **posizione e la forma** dell'oggetto o della caratteristica di interesse. Un'informazione che una cella robotizzata o una macchina automatica può usare direttamente per selezionare, prelevare, scartare o correggere.

- **Selezione e smistamento.** Sulle linee di riciclo il sistema localizza e classifica le diverse tipologie di plastica che scorrono sul nastro, fornendo al sistema di smistamento l'informazione su che cosa separare e dove.
- **Ambienti non controllati.** Lo stesso approccio lavora all'aperto, su macchine agricole, con polvere, vibrazioni e luce solare variabile. Fuori dalla fabbrica nulla è controllato: è il test più severo per la robustezza della percezione.
- **Macchine che si adattano.** Per i costruttori di macchine e di celle robotizzate, il cambio formato diventa un nuovo prompt invece che un nuovo progetto di visione, e la macchina può essere consegnata con la percezione già inclusa.

7. Revamping e add-on: nuova vista per gli impianti esistenti

La percezione zero-shot non è riservata alle macchine nuove. Gran parte del parco installato nell'industria italiana è fatto di linee, celle robotizzate e sistemi di visione che funzionano bene dal punto di vista meccanico, ma che faticano a stare al passo con prodotti sempre più vari. Sostituirli è costoso; riaddestrarli a ogni cambio formato, spesso, non è nemmeno possibile.

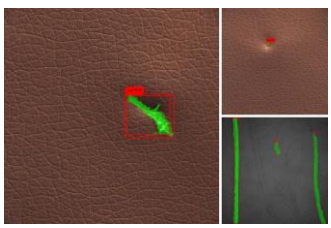
Può essere introdotta come **add-on** o all'interno di un progetto di **revamping**, affiancando o potenziando ciò che già c'è:

- **Integrazione non invasiva.** Il dispositivo edge si installa accanto alla linea o a bordo macchina e, dove possibile, sfrutta le telecamere già presenti. L'esito dell'ispezione viene restituito al PLC, al controllore del robot o al sistema di scarto esistente, senza riprogettare l'impianto.
- **Potenziare la visione esistente.** I sistemi di visione tradizionali, basati su regole e soglie, restano efficaci sui controlli dimensionali e ripetitivi. Il modello zero-shot si affianca a loro sui casi in cui faticano: superfici naturali, difetti dalla forma imprevedibile, prodotti nuovi o variabili.
- **Robot che vedono di più.** Una cella robotizzata esistente può acquisire la capacità di riconoscere oggetti e caratteristiche mai visti prima, ampliando i compiti che può svolgere senza cambiare la meccanica.
- **Investimento protetto.** Il revamping allunga la vita utile di macchine e linee e ne aumenta la flessibilità, con un intervento mirato invece di una sostituzione completa.

In questo senso un modello zero-shot non è solo un sistema di ispezione: è un **nucleo di percezione** riutilizzabile, pensato per dare a robot e automazione la capacità di "vedere" in modo generale, come farebbe una persona, in contesti che cambiano.

8. Sul campo: un modello, molti settori

Non una dimostrazione di laboratorio: lo stesso modello, senza essere riaddestrato né avere un dataset dedicato, è applicato oggi a materiali e settori che non hanno nulla in comune. Alcuni casi rappresentativi, descritti senza riferimenti ai clienti per riservatezza.

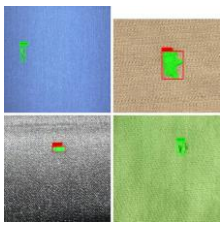


01 · CONCIA E PELLETTERIA

Ispezione pelli

La pelle è una delle superfici più difficili per la visione artificiale: la grana naturale cambia da pelle a pelle, quindi non esiste un "normale" fisso da imparare.

Il sistema rileva punture, rose, grinze, tagli, macchie, imperfezioni naturali e variazioni di colore o texture, e ne classifica la severità. Il risultato abilita una selezione e un taglio ottimizzati, riducendo lo spreco di un materiale pregiato.

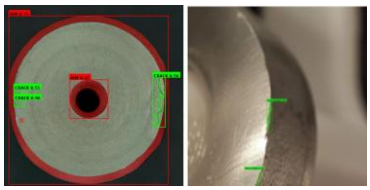


02 · TESSILE E ABBIGLIAMENTO

Ispezione tessuti

Rilevamento in linea di fori, strappi, difetti di trama e ordito, macchie, variazioni di colore e irregolarità di tessitura.

Le soglie di tolleranza sono regolabili dal cliente: tramite l'interfaccia agentica l'operatore può chiedere di essere più tollerante sulle piccole variazioni cromatiche, senza toccare il modello.



03 · MANIFATTURA E METALWORKING

Componenti meccanici

Ispezione in tempo reale di ruote dentate, bulloni e componenti di precisione per individuare filettature danneggiate, bave e imperfezioni superficiali.

Il controllo avviene direttamente in linea, riducendo scarti, rilavorazioni e fermi produzione.

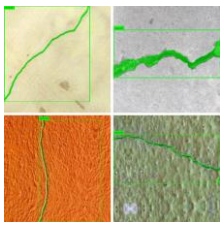


04 · AUTOMOTIVE

Monitoraggio cerchioni

Analisi di cerchioni, e più in generale di pezzi meccanici, per rilevare graffi, segni superficiali e deformazioni visibili.

Ogni difetto è localizzato e classificato con il relativo grado di confidenza, per un controllo qualità immediato a bordo linea.

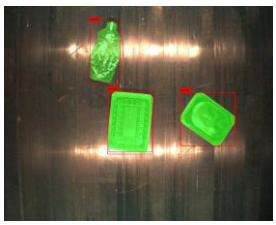


05 · LAVORAZIONE MATERIALI

Superfici di legno, acciaio e pietra

Rilevamento di nodi, graffi, porosità, crepe e variazioni cromatiche o di texture su superfici naturali e tecniche.

La segmentazione segue il difetto lungo tutta la sua estensione, anche quando ha forma irregolare, come nel caso di una crepa.



06 · RICICLO

Selezione delle plastiche

Sulle linee di riciclo il sistema localizza e classifica i diversi oggetti in plastica sul nastro, in condizioni di illuminazione difficili e anche con oggetti schiacciati o deformati.

L'output di segmentazione può guidare direttamente il sistema di smistamento automatico.

9. Che cosa cambia, e per chi

0	1	0
immagini etichettate e cicli di training per avviare l'ispezione	prompt per ogni cambio prodotto	immagini che lasciano l'azienda

Tempo. I tempi di messa in servizio non dipendono più dalla raccolta dei dati, ma dall'integrazione meccanica e ottica: le caratteristiche rilevanti si individuano sui primi pezzi, in ore anziché in mesi.

Flessibilità. Un cambio di prodotto è un nuovo prompt, non un nuovo progetto. Il sistema gestisce la variabilità delle condizioni operative (illuminazione, angolazioni, materiali, configurazioni di linea) senza ricalibrare il modello ambiente per ambiente.

Competenze. Non serve un team di data science dal lato del cliente: la data science è fatta una volta, a monte. Contano invece le competenze di chi conosce il processo e il prodotto, e di chi sa portare la visione dentro la macchina.

Controllo del dato. L'elaborazione avviene interamente on-premise. Le immagini di prodotto, che spesso contengono know-how industriale riservato, non escono dallo stabilimento.

10. Perché conta per l'industria

Il dibattito sull'adozione dell'intelligenza artificiale nell'industria incontra spesso gli stessi ostacoli: la scarsità di competenze specialistiche, soprattutto nelle piccole e medie imprese, il costo e la lentezza dei progetti basati sui dati, la difficoltà di passare dal pilota alla produzione. L'esperienza di Awentia suggerisce che una parte di questi ostacoli dipende meno dalla tecnologia in sé che dal **modo in cui viene confezionata**.

Spostare il lavoro di data science a monte, una volta per tutte, e lasciare al cliente solo la descrizione di che cosa cercare significa rendere l'AI accessibile anche a chi non ha, e non avrà, un team dedicato. È un modello particolarmente adatto alle produzioni in cui la varietà di prodotto e la qualità dei materiali sono un vantaggio competitivo che i sistemi rigidi tendono a penalizzare.

C'è poi un tema di **controllo e sovranità del dato**. In una fase in cui la mappa mondiale dell'AI e le sue implicazioni geopolitiche sono al centro dell'attenzione, un'architettura edge e on-premise consente di adottare modelli fondazionali avanzati senza trasferire immagini e know-how di processo fuori dallo stabilimento, e senza dipendere da una connessione costante a infrastrutture cloud esterne.

> *La domanda per il settore non è più se l'AI funzioni in fabbrica, ma come renderla configurabile da chi la fabbrica la conosce.*

11. Chi è Awentia Vision Technologies

Awentia Vision Technologies, con sede a Imola, supera i limiti della computer vision rigida con un approccio di **Intelligent Physical Automation**, pensato per gli ambienti ad alta variabilità e poco prevedibili dell'industria moderna. Al centro c'è una **percezione di tipo umano** (*human-like perception*): come un operatore esperto riconosce un difetto o un oggetto anche su un prodotto che non ha mai visto, così i sistemi Awentia, grazie allo **Zero-Shot Learning**, riconoscono oggetti e caratteristiche mai visti prima a partire da descrizioni semantiche. Questo elimina il collo di bottiglia dell'annotazione e i costi dell'etichettatura manuale dei dati. Un'architettura **edge-native** elabora i dati direttamente in sede, con risposte in tempo reale compatibili con i cicli macchina e la piena sovranità del cliente sui propri dati. L'obiettivo è uno: **dare a macchine e robot la capacità di vedere come una persona**, capendo che cosa conta anche davanti a ciò che non hanno mai visto.

Awentia è associata ad **AIdAM** e collabora con costruttori di macchine, system integrator e partner tecnologici per portare la percezione zero-shot direttamente all'interno di macchine e linee di produzione.

12. I nostri riferimenti per contattarci

Metti alla prova la percezione zero-shot sui tuoi pezzi, sulla tua linea. Scrivici per richiedere una **demo gratuita** o per raccontarci la tua sfida di visione:

AZIENDA	Awentia Vision Technologies · Imola
SITO WEB	ai-core.awentia.com
E-MAIL	info@awentia.com
LINKEDIN	linkedin.com/company/awentia

Case History 2 – HumanQ Srl[4]

1. Introduzione: il limite del modello "più potenza, più possibilità"

Per oltre quarant'anni l'evoluzione dell'informatica ha seguito un paradigma sostanzialmente lineare: per affrontare problemi di dimensione maggiore era sufficiente disporre di hardware più performante. L'aumento della frequenza di clock, la moltiplicazione dei core, l'adozione delle GPU come acceleratori general purpose, la diffusione del cloud computing e, più di recente, delle infrastrutture HPC hanno reso trattabili carichi di lavoro che fino a pochi anni prima risultavano proibitivi. Dalla simulazione ingegneristica all'analisi finanziaria, dalla computer grafica 3D all'Intelligenza Artificiale, l'intera economia digitale si è sviluppata secondo questo modello: incrementare la capacità di calcolo per ampliare lo spazio dei problemi risolvibili.

Oggi questo approccio, pur restando fondamentale, mostra un limite strutturale. La ragione non è un rallentamento del progresso hardware: le risorse disponibili sono le più elevate mai raggiunte. Ciò che è cambiato è la natura dei problemi. Per lungo tempo l'obiettivo prevalente è stato l'elaborazione di grandi volumi di dati nel minor tempo possibile (throughput). Sempre più spesso, invece, il problema consiste nel prendere decisioni ottimali in scenari ad elevata complessità. E la complessità non scala come il volume dei dati: segue leggi di crescita ben diverse, tipicamente combinatorie o esponenziali rispetto al numero di variabili in gioco.

La gestione, l'analisi e l'estrazione di valore da dataset massivi pongono quindi sfide senza precedenti alle architetture di calcolo classico. GPU e sistemi HPC hanno esteso i confini computazionali, ma la complessità intrinseca di molti problemi di ottimizzazione e di machine learning resta un ostacolo rilevante.

2. Calcolo quantistico, era NISQ ed emulazione

In questo contesto il Quantum Computing si delinea come il cambio di paradigma necessario. Tuttavia, i processori quantistici fisici attuali, appartenenti all'era NISQ (Noisy Intermediate-Scale Quantum), sono affetti da elevati tassi di decoerenza e da rumore quantistico, che limitano l'implementazione pratica di algoritmi complessi su larga scala. Per colmare il divario tra la teoria algoritmica quantistica e la disponibilità di hardware stabile, gli emulatori quantistici eseguiti su supercomputer classici rappresentano uno strumento essenziale per la sperimentazione avanzata sui Big Data.

---

[4] A cura di HumanQ Srl e in collaborazione con il Prof. Marco Armoni, fondatore di MCG S.r.l.

È in questo scenario che HumanQ S.r.l., affiancata da MCG S.r.l. (Media Connect Group S.r.l.), conduce un'intensa attività di sviluppo, diffusione e promozione di tecnologie di emulazione quantistica denominate EQM (Emulation Quantum Machinery). Tali tecnologie consentono di studiare algoritmi, modelli computazionali e strategie di ottimizzazione senza attendere la piena maturità dell'hardware quantistico. Occorre precisare che l'EQM non si propone come alternativa al Quantum Computing, ma come strumento che permette a ricercatori, università, imprese e PA di acquisire fin da subito dimestichezza con un paradigma destinato a influenzare profondamente l'evoluzione dell'informatica.

Il tratto distintivo del nostro approccio consiste nell'operare all'intersezione tra ricerca accademica e innovazione industriale, grazie alla collaborazione con istituzioni come il Centro Italiano di Emulazione Quantistica e alla sinergia con MCG S.r.l., che consente di integrare competenze multidisciplinari e know-how ingegneristico. Ne derivano nuove modalità di trattazione di problemi complessi, tra cui l'adozione di modelli ibridi classico-quantistici, con ricadute concrete in comparti in trasformazione quali l'aerospaziale, l'agroalimentare, l'ambientale, il manifatturiero, il sanitario e molti altri.

3. La complessità computazionale: esempio applicativo

Si consideri un'azienda manifatturiera che debba pianificare la produzione di decine di stabilimenti dislocati in diversi Paesi. Ciascun impianto presenta capacità produttive differenti, ciascuna linea utilizza materiali forniti da fornitori diversi, ciascun mercato esprime requisiti specifici e ogni ritardo si propaga lungo l'intera supply chain. A queste variabili si sommano i costi energetici, la disponibilità delle materie prime, le condizioni meteorologiche, le tensioni geopolitiche, i vincoli normativi ambientali e la dinamica della domanda.

La raccolta delle informazioni non costituisce il collo di bottiglia: le organizzazioni vi provvedono già. Il problema è individuare, tra tutte, la combinazione di decisioni che produce il risultato migliore. Ogni variabile aggiuntiva amplia l'insieme delle alternative, ogni alternativa genera ulteriori ramificazioni e, già con poche decine di parametri, lo spazio delle soluzioni diventa troppo esteso per essere esplorato in modo esaustivo con gli strumenti tradizionali. È questo il significato di complessità computazionale: non una difficoltà di comprensione del problema, ma una crescita del numero di soluzioni candidate molto più rapida della capacità di valutarle singolarmente.

Lo stesso fenomeno si osserva in domini eterogenei. Nella pianificazione delle reti elettriche, dove migliaia di generatori, sistemi di accumulo e punti di consumo devono essere coordinati in tempo reale. Nella gestione del traffico urbano, dove milioni di spostamenti quotidiani alterano continuamente l'equilibrio della rete stradale. In ambito sanitario, dove allocazione delle risorse,

pianificazione delle attività cliniche e gestione delle emergenze impongono decisioni rapide in presenza di un numero molto elevato di variabili.

Anche la cybersecurity si colloca oggi nella stessa condizione. Per molti anni è stata interpretata come un problema prevalentemente tecnologico, affrontabile con firewall, antivirus aggiornati, segmentazione di rete e regole di accesso progressivamente più sofisticate. Tali misure restano necessarie ma non sono più sufficienti. Le organizzazioni devono analizzare in modo continuo migliaia di eventi, correlare informazioni provenienti da sistemi eterogenei, valutare il comportamento degli utenti, comprendere il contesto operativo, anticipare l'evoluzione delle minacce e decidere in tempi estremamente ridotti. Anche in questo caso il vincolo non è la scarsità di dati, ma l'enorme numero di scenari da valutare prima di selezionare la risposta più efficace.

4. Dall'elaborazione dei dati al supporto alle decisioni

Questa trasformazione sta ridefinendo il ruolo dell'informatica. Per decenni abbiamo progettato sistemi orientati soprattutto all'elaborazione dell'informazione; oggi servono sistemi in grado di supportare i processi decisionali. La distinzione è tutt'altro che marginale: elaborare significa trasformare dati, decidere significa esplorare uno spazio di possibilità, e tale esplorazione richiede modelli computazionali differenti.

In questo quadro convergono alcune delle tecnologie più rilevanti del nostro tempo. L'Intelligenza Artificiale consente di individuare correlazioni difficilmente riconoscibili dall'analisi umana e di costruire modelli predittivi sempre più sofisticati. La simulazione permette di rappresentare digitalmente processi complessi e di verificarne il comportamento prima dell'applicazione nel mondo reale. La ricerca operativa sviluppa algoritmi per l'ottimizzazione di sistemi con milioni di variabili. La cybersecurity evolve verso modelli adattivi, in cui la protezione dipende dalla capacità di interpretare il contesto e non dalla sola applicazione di regole statiche. Parallelamente, il Quantum Computing e l'emulazione quantistica aprono nuove prospettive nello studio di problemi caratterizzati da una crescita combinatoria estremamente elevata.

Queste tecnologie non sono in competizione: costituiscono i tasselli di un unico ecosistema. L'errore più frequente consiste nel ritenere che il Quantum Computing sostituirà i computer tradizionali, oppure che l'Intelligenza Artificiale renderà obsolete le altre discipline. L'evoluzione storica dell'informatica indica il contrario: ogni nuova tecnologia si affianca a quelle esistenti, ne amplia le possibilità e genera nuovi modelli di integrazione.

Lo stesso principio guida l'EQM, il cui obiettivo è realizzare un ambiente di ricerca e sperimentazione che renda accessibili concetti, algoritmi e modelli computazionali ispirati al

paradigma quantistico, sfruttando le moderne architetture CPU e GPU. In altri termini, un ponte tra l'informatica attuale e quella che, progressivamente, caratterizzerà il prossimo decennio.

5. Use cases

L'obiettivo primario della tecnologia EQM non è quello di sostituire gli algoritmi classici, ma è quello di individuare problemi nei quali l'esplosione combinatoria, l'ottimizzazione multicriterio o la necessità di rivalutare rapidamente molte alternative rendono utile una diversa rappresentazione del problema.

Il principio comune, che è alla base dell'architettura concettuale, è così strutturato: i dati reali e i vincoli vengono trasformati in un modello che viene, a sua volta, codificato nello spazio quantistico. L'elaborazione modifica le ampiezze associate agli stati e, infine, misura e decodifica riportano il risultato nel dominio applicativo.

Le presentazioni EQM descrivono una piattaforma GPU-based con emulazione a vettore di stato, esecuzione parallela delle operazioni, backend OpenCL e possibilità di scalare da problemi più piccoli a scenari più ampi. La catena architetturale separa gli input applicativi dalla codifica del modello, dal motore di emulazione e dall'estrazione del risultato.

Con n qubit, il registro quantistico è descritto in uno spazio di dimensione 2^n. Dunque, a titolo esemplificativo, a 22 qubit, lo spazio comprende 4.194.304 stati base. Questo numero è fondamentale per comprendere la scala dei casi d'uso: non rappresenta 4.194.304 record letti come in un database, ma 4.194.304 componenti del vettore di stato sulle quali agiscono le trasformazioni quantistiche.

La computazione quantistica diventa interessante per un'organizzazione quando può essere collegata a un problema reale. A supporto di quanto sopra, sono stati sviluppati dei casi d'uso in ambito sanitario, logistico urbano e strategico caratterizzati da domini diversi, ma legati da un aspetto essenziale: decisioni che dipendono da molte variabili, molti vincoli e un numero di configurazioni che cresce rapidamente.

EQM consente di rappresentare queste configurazioni in uno spazio quantistico emulato e di utilizzare tale rappresentazione come motore computazionale integrabile nelle applicazioni.

5.1 Sanità

Il caso sanitario che è stato sviluppato affronta decisioni che coinvolgono milioni di pazienti, diverse caratteristiche cliniche e numerose strategie terapeutiche. Nello specifico, il modello di

riferimento considerava 5.000.000 di pazienti, 16 variabili cliniche e 128 protocolli terapeutici. Ogni alternativa è stata valutata rispetto a più obiettivi: dati demografici, dati clinici, storicità, efficacia, rischio clinico, costi operativi, occupazione delle risorse ospedaliere e sostenibilità del sistema. Questi obiettivi hanno tenuto conto di caratteristiche della popolazione e segmentazione, condizioni e indicatori clinici, informazioni cliniche pregresse, probabilità di successo del protocollo, rischio associato alla scelta di protocollo, impatto economico di quest'ultimo, impiego delle risorse ospedaliere e relative capacità e, infine, impatto complessivo sul sistema sanitario. Successivamente, all'interno del modello quantistico, ad ognuno degli obiettivi sopra descritti è stato assegnato un ruolo matematico che racchiude e definisce il profilo del singolo paziente, la caratterizzazione dello stato, i contesti per compatibilità e rischio, criteri di massimizzazione, riduzione, ottimizzazione e vincoli/obiettivi del sistema. Una volta terminata la fase di modellazione e codifica dello spazio quantistico decisionale, è stato possibile fare eseguire al motore computazionale valutazioni, misurazioni ed infine estrazione dei dati, quali, ad esempio, il protocollo raccomandato da somministrare ai pazienti indagati.

Nel caso specifico sopra descritto, in cui sono stati analizzati 5.000.000 di pazienti, 16 variabili cliniche e 128 protocolli terapeutici, utilizzando una capacità di calcolo a 22 qubit logici (4.194.304 configurazioni valutare), il modello quantistico è stato in grado di restituire in output il protocollo T-038, quale soluzione migliore da adottare, in un tempo di 94 ms con un'indicazione del 99% di successo clinico.

5.2 Mobilità - Mobility Optimizer

Il caso di mobilità urbana elaborato, fa riferimento ad una città di 5.000.000 di cittadini, 50.000 veicoli, 1.000 incroci e 10.000 semafori. Nella fattispecie, nel caso d'uso si tiene conto anche del trasporto pubblico, dei parcheggi, di eventi cittadini e di emergenze.

L'obiettivo del modello di calcolo è stato quello di produrre piani coordinati finalizzati alla riduzione della congestione del traffico e ai tempi di percorrenza, all'ottimizzazione del trasporto pubblico, al miglioramento della risposta alle emergenze e alla riduzione delle emissioni di CO_2.

In particolare, per ognuno dei fattori presi in considerazione, sono stati valutati e considerati diversi aspetti quali la scala complessiva della domanda urbana, i flussi e pressione sulla rete stradale, la topologia urbana e i punti di "decisione", i piani semaforici ed il relativo coordinamento, l'ottimizzazione delle linee di trasporto e la frequenza delle corse, la gestione intelligente delle soste dei veicoli nei parcheggi, le variazioni dinamiche della domanda/capacità in occasione di manifestazioni, concerti, eventi e lavori ed, infine, i percorsi e priorità legati alle operazioni di interventi in emergenza.

Anche in questo caso, tutte le variabili sopra descritte sono state modellate e codificate all'interno dello spazio quantistico decisionale, consentendo al motore di calcolo in emulazione di restituire una serie di KPI inerenti allo scenario ottimizzato. In particolare, il piano di ottimizzazione della mobilità generato ha comportato una riduzione della congestione del traffico del 55%, una riduzione dei tempi di percorrenza del 45%, una riduzione delle emissioni di CO2 del 30%, un miglioramento della risposta negli interventi di emergenza del 50%, un miglioramento del trasporto pubblico del 40% ed un incremento dalla disponibilità dei parcheggi del 35%.

5.3 Difesa - Strategic Planner

Il caso Strategic Planner, sviluppato per il settore difesa, affronta la pianificazione in un ambiente multidominio dinamico, con minacce simultanee, risorse limitate e vincoli operativi. I materiali descrivono uno scenario con incursione terrestre, sciame di droni e sabotaggio cyber, nel quale il decisore deve allocare risorse e adattare il piano non appena le condizioni cambiano.

In questo contesto è stato fondamentale individuare le categorie principali e le rispettive funzioni, tra cui Intelligence e ISR, intesi come informatori e sorveglianza, designati all'aggiornamento dello scenario, dati operativi, intesi come stato delle operazioni, per la definizione del contesto, Feed delle minacce (terresti, aeree, marittime e cyber) necessarie per la definizione delle variabili dinamiche, logistica ed asset disponibili per comprendere capacità e allocazione delle risorse, regole e vincoli, legati a priorità, limiti e regole d'ingaggio, necessari per la definizione dello spazio ammissibile, tempo nel quale risiede il vincolo decisionale, rischio, inteso come rischio per le forze e rischio collaterale, valutato secondo un metodo multicriterio ed, infine, le dipendenze che supportano la coerenza del piano tenendo in conto le interdipendenze tra domini e risorse.

Definendo uno scenario caratterizzato da una batteria di difesa aerea composta da 6 unità, un cyber team di 4 risorse, un asset ISR (*Intelligence, Surveillance, and Reconnaissance*) composto da 5 unità, 3 unità di forze speciali, 6 unità logistiche e 4 unità navali, il verificarsi di un potenziale evento critico modifica il contesto attivando, di conseguenza, un ciclo di ripianificazione. Nella fattispecie, il modello computazionale ha restituito in circa 2 secondi la migliore strategia di ripianificazione che ha aumentato del 76% la capacità di neutralizzazione della minaccia, ha ridotto del 68% i tempi di risposta e, dunque, di reazione, ha incrementato le probabilità di successo del 58% ed ha incrementato l'efficienza delle risorse del 34%.

Lo scenario sopra descritto è stato strutturato in modo da funzionare in maniera continuativa, effettuando acquisizione di dati, aggiornamento del modello computazionale, ri-ottimizzazione,

elaborazione ed esecuzione del piano ciclicamente, consentendo al modello un adattamento dinamico compatibile con l'aggiornamento dello scenario.

6. Conclusioni

La descrizione dei tre casi applicativi mostra che la tecnologia EQM non dipende semanticamente dal dominio. Cambiano i dati, i vincoli e la funzione obiettivo mentre resta stabile la struttura: ingestione dei dati, costruzione dello spazio decisionale, codifica, emulazione, analisi e traduzione del risultato.

I casi d'uso mostrano concretamente perché l'emulazione quantistica può essere interessante prima ancora della disponibilità diffusa di QPU fault-tolerant. Il punto di partenza è la complessità: milioni di soggetti o eventi, decine di variabili, centinaia di alternative, reti urbane estese o scenari multidominio. EQM trasforma questi elementi in uno spazio computazionale nel quale possono essere applicate logiche quantistiche e dal quale viene estratto un risultato nuovamente comprensibile al software e al decisore.

Nella Sanità il risultato è una raccomandazione fra protocolli valutati secondo criteri clinici e di sistema. Nella Smart City è un insieme coordinato di piani per semafori, routing, emergenze, trasporto pubblico e parcheggi. Nella Difesa è un piano di allocazione e una capacità di ripianificazione quando cambiano minacce e vincoli. Tre domini diversi, quindi, ma una medesima idea architetturale: trasformare uno spazio decisionale complesso in una rappresentazione quantistica emulata e riportare l'elaborazione nel processo applicativo.

Il Quantum rappresenta una delle possibili risposte a questa evoluzione, ma il cambiamento di fondo è culturale prima ancora che tecnologico: significa superare la concezione del computer come mero strumento di elaborazione e considerarlo una piattaforma di supporto alle decisioni, che dipendono da numerose variabili, numerosi vincoli e da un numero di configurazioni in rapida crescita.

In questa direzione si colloca il nostro lavoro: l'EQM consente di rappresentare tali configurazioni in uno spazio quantistico emulato e di utilizzare questa rappresentazione come motore computazionale integrabile nelle applicazioni.

L'interesse di EQM non è mostrare il quantum computing come esercizio teorico, ma renderlo un livello computazionale utilizzabile per costruire e sperimentare applicazioni reali.

AZIENDA	HumanQ · Brescia
SITO WEB	www.humanq.it
E-MAIL	info@humanq.it
LINKEDIN	https://www.linkedin.com/company/human-q/