

Intelligenza Artificiale
(quali novità?)

Angelo Giorgetti - Maurizio Parini

Conviviale Rotary Club Porta Vercellina, Milano 18-03-2024

L’informatica oggi, de facto …

UN VASTO INSIEME DI TEMATICHE raffigurabili come

cambiamento *(epocale)* — *nella dimensione SOCIO-ECONOMICA*

evoluzione *(esponenziale)* — *nella dimensione TECNOLOGICA*

complessità *(emergente)* — *nella dimensione SCIENTIFICA*

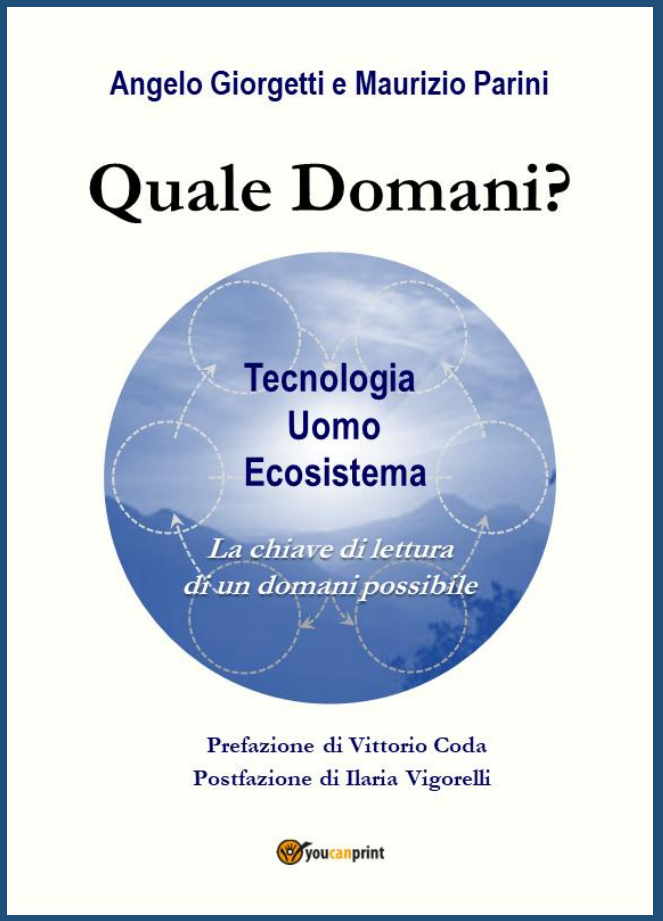
Una chiave di lettura complessiva

… da un'esperienza
(condivisa con molte persone)





… e da una riflessione
(condivisa con molte persone)

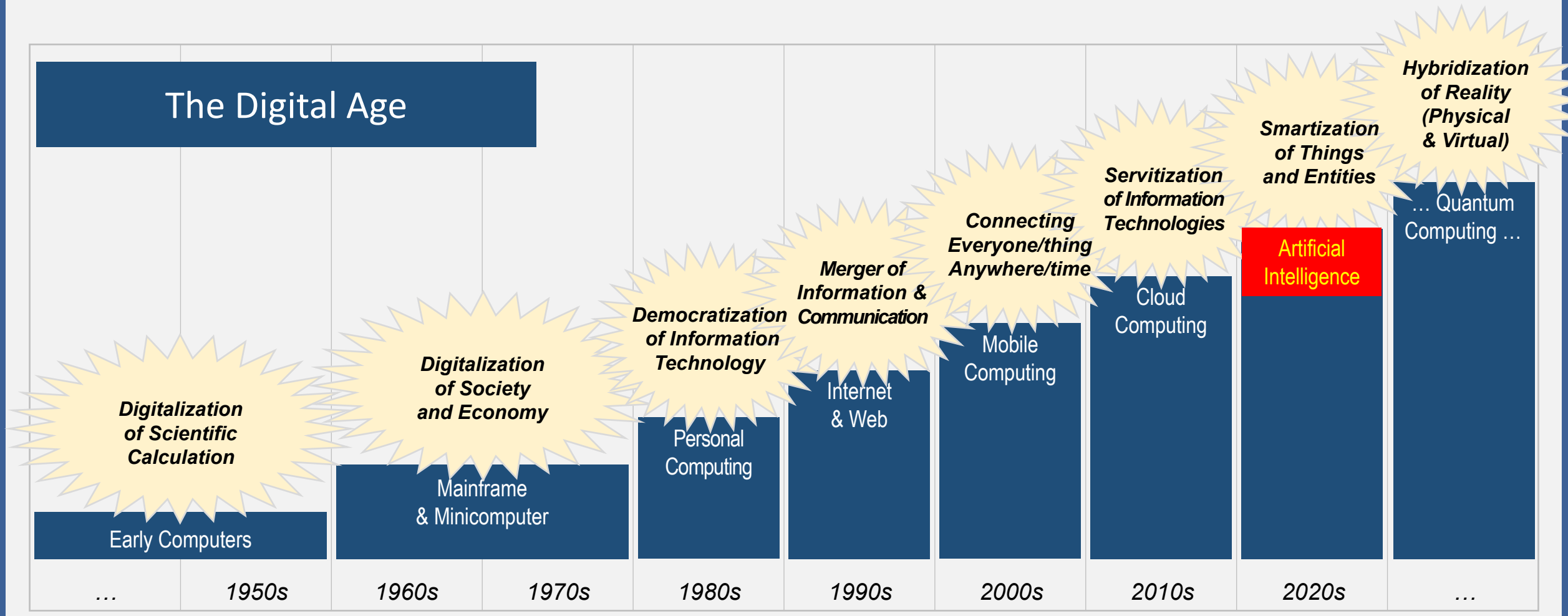


In primo piano, oggi …

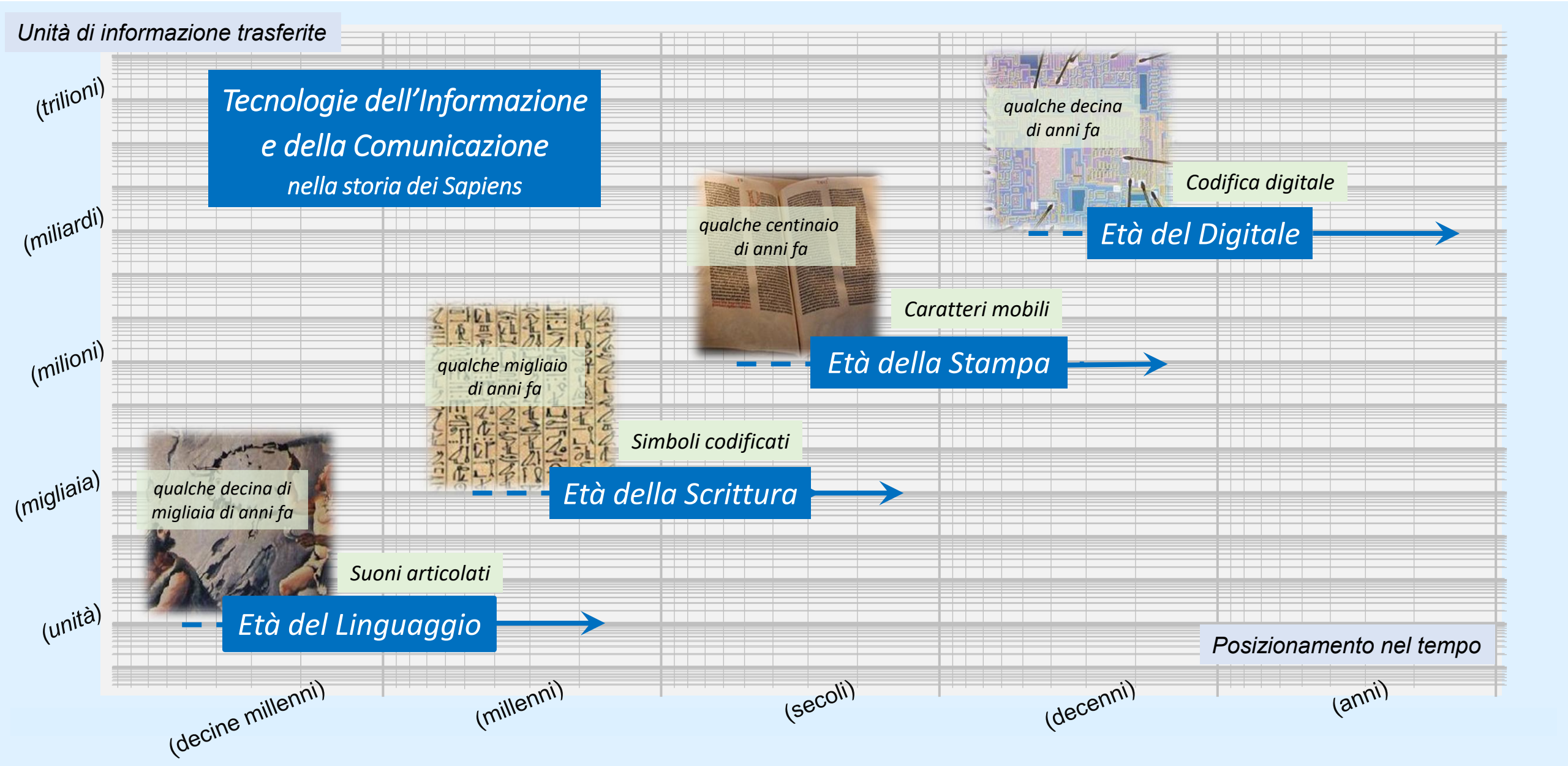


Tecnologie Informatiche: evoluzione e cambiamento indotto

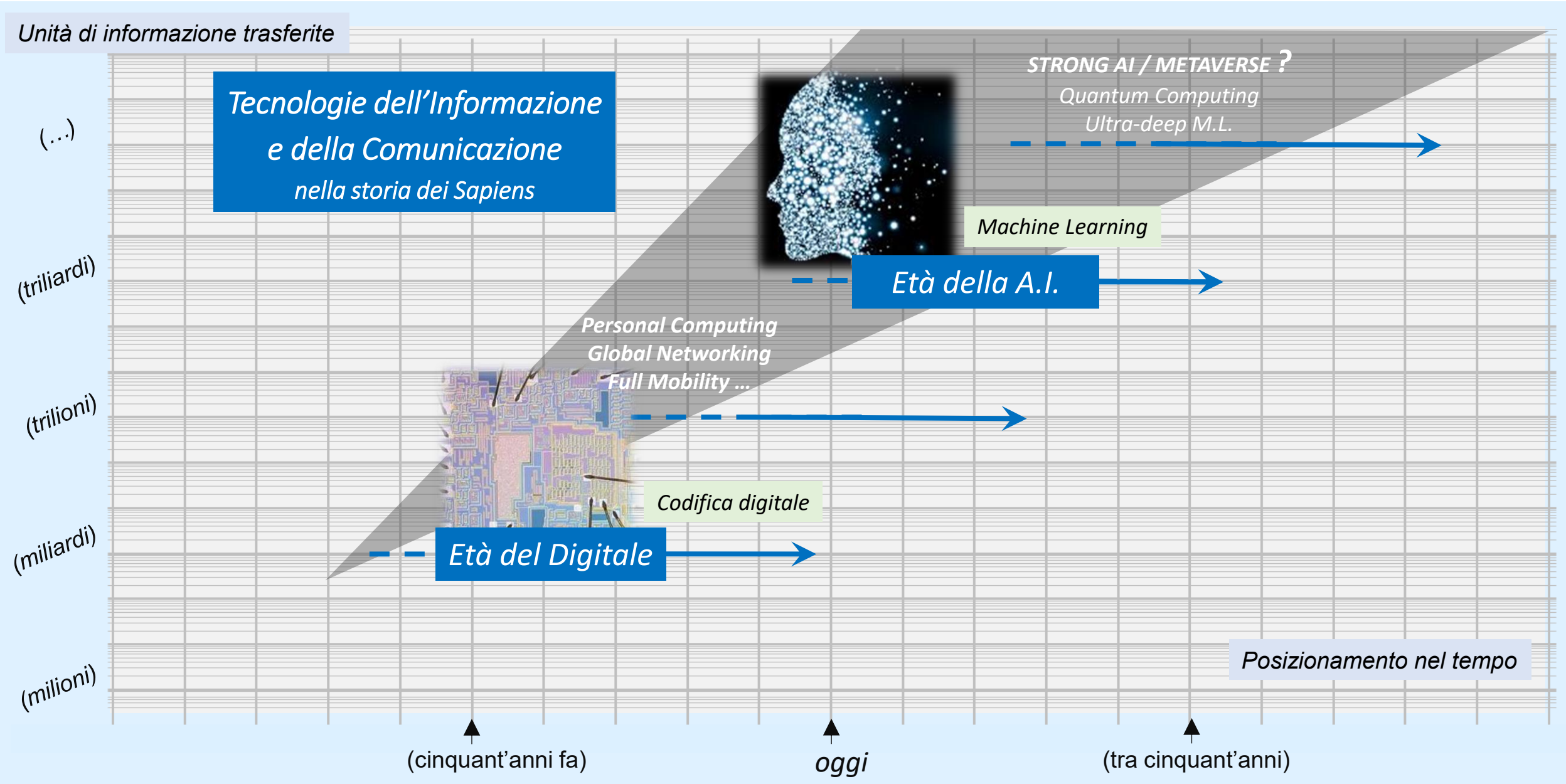
(ChatGPT docet …)



Un cambiamento epocale…



… concentrato nella durata di una generazione



Un cambiamento «esponenziale» e sempre più «pervasivo» …

Evoluzione e Convergenza Tecnologie

…
web3
trust architectures and dig. identity
quantum technologies
industrializing machine learning
immersive-reality technologies
applied AI
…
artificial intelligence…
big data/analytics
M2M, H2M e M2H comm.
cloud & edge computing
advanced sensors
…
bitcoins
e-commerce
social media
smart phone
search engine
arpanet
world wide web
pc
minicomputer
mainframe
…

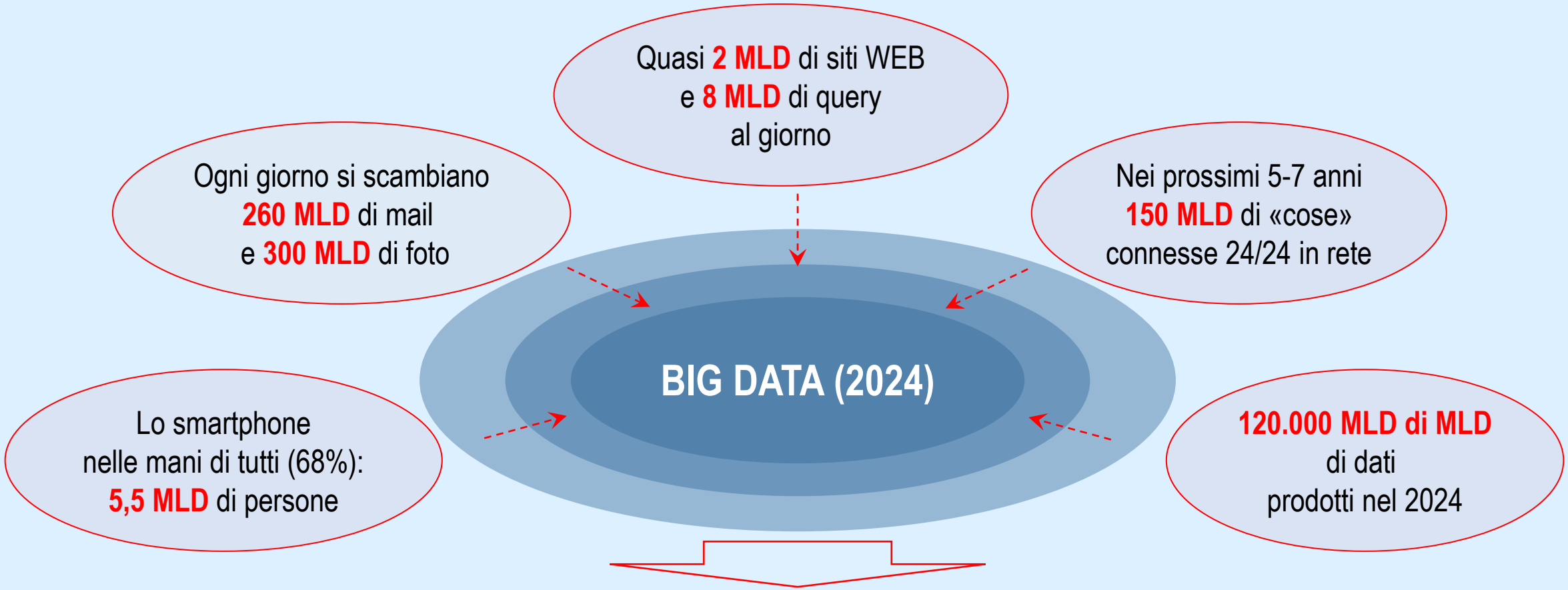
Presente del futuro
tutto diventa … «Hybrid»
Augmented and Virtual Realities

Presente del presente
tutto diventa … «Smart»
Intelligent and Connected Things

Presente del passato
tutto diventa … «Digital»
Professional, Personal and Social Tools



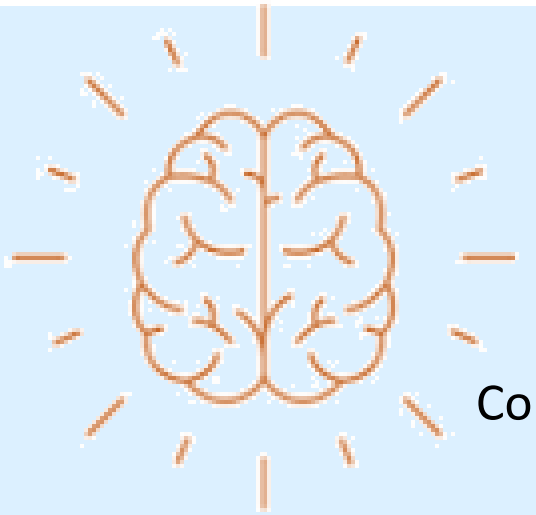
tutto diventa … «Smart»: lo tsunami dei dati



Tempo di raddoppio (*)
7 mesi nel 2022
12 ore nel 2030

(*) tempo nel quale viene prodotto lo stesso numero di dati prodotti dall'inizio della civiltà

Intelligenza



Qualità mentale
che consiste nella capacità di
apprendere dall'esperienza,
adattarsi a nuove situazioni,
comprendere e gestire concetti astratti
e usare la conoscenza per manipolare il
proprio ambiente

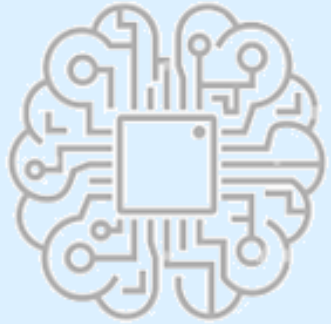
(Encyclopedia Britannica)

Complesso di facoltà psichiche e mentali
che consentono di pensare,
comprendere o spiegare i fatti o le azioni,
elaborare modelli astratti della realtà,
intendere e farsi intendere dagli altri,
giudicare,
e adattarsi all’ambiente

(Enciclopedia Treccani)

Intelligenza Artificiale: definizioni a fini divulgativi (suggestioni)

« … la capacità di un sistema informatico di eseguire compiti che normalmente richiedono l'intelligenza umana …»



«… sistemi informatici che dimostrano un'intelligenza simile a quella umana e capacità cognitive, come la deduzione, il riconoscimento di modelli e l'interpretazione di dati complessi …»

Intelligenza artificiale ristretta (ANI)

- nota anche come *AI debole*
- una forma di IA che ha funzionalità limitate a compiti limitati
- più efficiente degli esseri umani nell'esecuzione di un numero specifico o limitato di compiti
- **è l'unico tipo di IA che esiste oggi**

Intelligenza artificiale generale (AGI)

- nota anche come *AI forte*
- una forma di AI che possiede capacità di generalizzazione
- stesso livello di capacità degli esseri umani di adattarsi a situazioni diversificate
- **realizzazione ancora molto lontana**

Super intelligenza artificiale (ASI)

- forma di *AI forte* diversa da AGI
- significativamente più potente di quella degli esseri umani sotto tutti gli aspetti
- può dotare le macchine di bisogni, credenze e desideri propri
- **attualmente, l'ASI è solo teorica**

Intelligenza Artificiale: definizioni a fini politici (normativi)

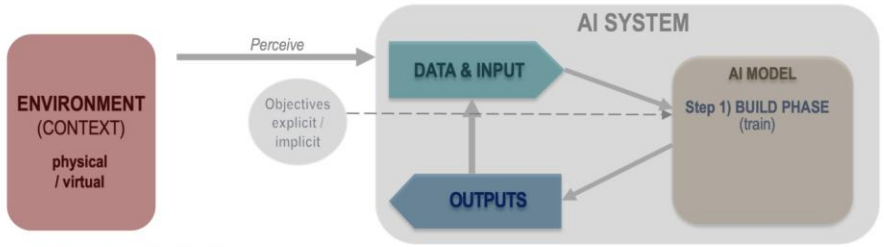
National artificial intelligence act — 2020

The term 'artificial intelligence' means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments

OCSE: Sistema di Intelligenza Artificiale (def.) — 2023 — *EU 2024*

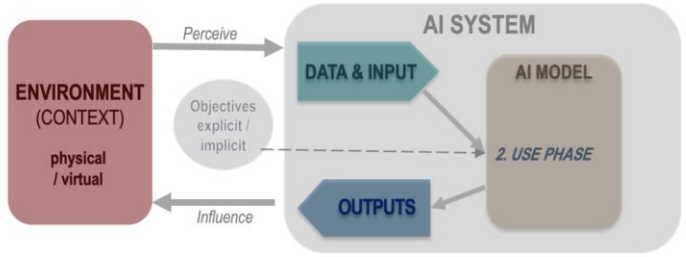
*An AI system is a machine-based system that, for **explicit or implicit** objectives, **infers, from the input it receives, how to generate outputs such as** predictions, **content**, recommendations, or decisions **that can** influence **physical** or virtual environments. **Different** AI systems vary **in their** levels of autonomy **and adaptiveness after deployment**»*

BUILD PHASE:
An AI system is a **machine-based** system, that



- for **explicit or implicit objectives**
- **infers**, from the **input** it receives
- How to **generate outputs** such as predictions, content, recommendations, or decisions

USE PHASE (once the model is built):
An AI system is a **machine-based** system, that



- for explicit or implicit objectives
- infers, from the input it receives
- How to generate outputs such as predictions, content, recommendations, or decisions
- **that [can] influence physical or virtual environments;**

Different AI systems vary in their levels of autonomy and adaptiveness [after deployment].

Intelligenza Artificiale: definizioni a fini marketing (speculativi)

Dopo circa 70 anni dalla coniazione del termine la definizione teorica di Intelligenza Artificiale resta ancora piuttosto vaga, senza confini semantici precisi e duraturi …

"… Da qualche tempo, le aziende del settore IT hanno battezzato (o ribattezzato) molti prodotti software come prodotti di Intelligenza Artificiale. La scelta li rende più appetibili al mercato, ma, nella realtà, non sempre questi prodotti sono realmente «AI-Powered» …"

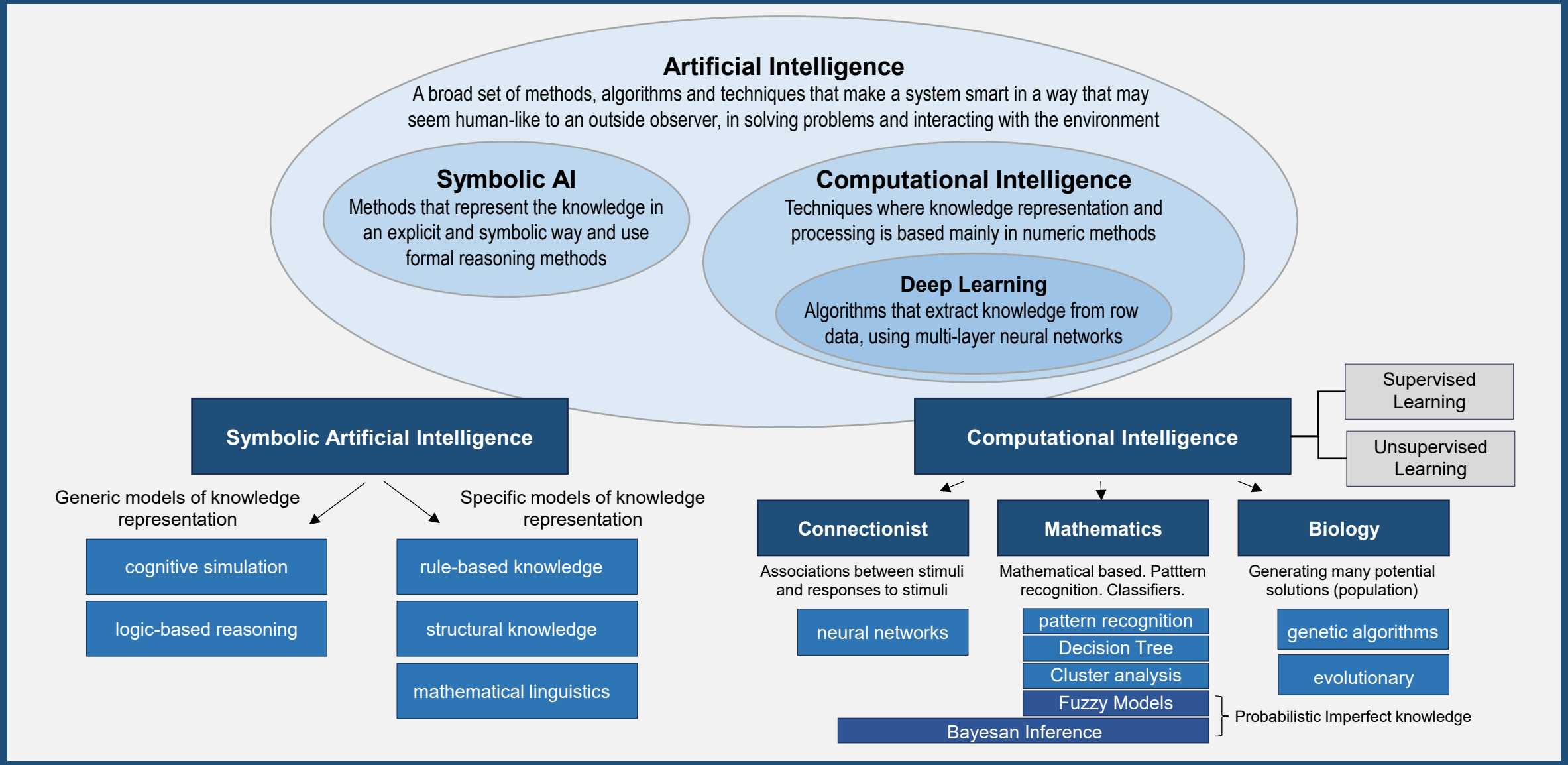
Per chi 'vende' soluzioni applicative di punta, Intelligenza Artificiale è …

Un software che integra al proprio interno algoritmi strutturati dinamicamente

- *per subire influenze da molteplici eventi esterni (sensori, dati, database, ecc.) ed interni (matching, data targeting, ecc.) che ne espandono il bagaglio di apprendimento*
- *così da generare spontaneamente nuove soluzioni sempre più raffinate, secondo il fine ultimo per cui è stato sviluppato il software e l'ambito d'applicazione dello stesso*

… e non sono Intelligenza Artificiale tutti i software a cui manca qualcosa di quanto sopra

Intelligenza Artificiale (tecnicamente)



Intelligenza Artificiale Simbolica

(a lungo la sola IA disponibile)

Nell'IA simbolica (SAI) gli oggetti sono rappresentati come simboli
e le loro relazioni descritte in un linguaggio formale che i computer possono manipolare

Un esempio di SAI sono i Sistemi Esperti

("un programma informatico intelligente che utilizza procedure di conoscenza e inferenza per risolvere problemi che sono abbastanza difficili da richiedere una significativa esperienza umana per la loro soluzione")

Utilizzano regole per fornire raccomandazioni in diversi campi (come la medicina)

Punto di forza della SAI è soprattutto
la trasparenza
(facile interpretare il modo in cui
giunge a una conclusione)

I limiti della SAI sono soprattutto
la mancanza di scalabilità
e di apprendimento autonomo
(richiede una conoscenza completa del dominio)

Intelligenza Computazionale (Machine Learning)

(già molto diffusa oggi in tutti i settori)

Sottoinsieme dell'AI che riguarda algoritmi e tecniche che consentono alle macchine di apprendere dai dati

Apprendimento supervisionato (SML)

- *'Machine' addestrata da un supervisore con utilizzo di dati etichettati (p.e., molti esempi di immagini di aerei etichettate come tali)*
- *La variabile di risultato o variabile target è nota (p.e.,aereo): la 'machine' deve identificarla con precisione in nuove immagini non etichettate*
- *Identificazione si basa su vari metodi statistici, principalmente*
  - *algoritmi di classificazione (quando la variabile di destinazione è categorica)*
  - *algoritmi di regressione (quando la variabile di destinazione è continua)*

Apprendimento non supervisionato (USML)

- *Non c'è un supervisore. La 'machine' è responsabile dell'analisi dei dati e della ricerca di modelli nei dati (p.e., i dati sono migliaia di immagini di frutti da raggruppare in categorie simili per forma, colore, dimensioni …)*
- *Viene utilizzato tipicamente per la 'riduzione delle dimensioni' o il riconoscimento di modelli*
- *Due le principali categorie di algoritmi nel USML:*
  - *clustering (insieme di algoritmi utilizzati per raggruppare i dati non etichettati in diverse categorie)*
  - *associazione (algoritmi basati su regole utilizzati per trovare le associazioni tra dati diversi in un set di dati)*

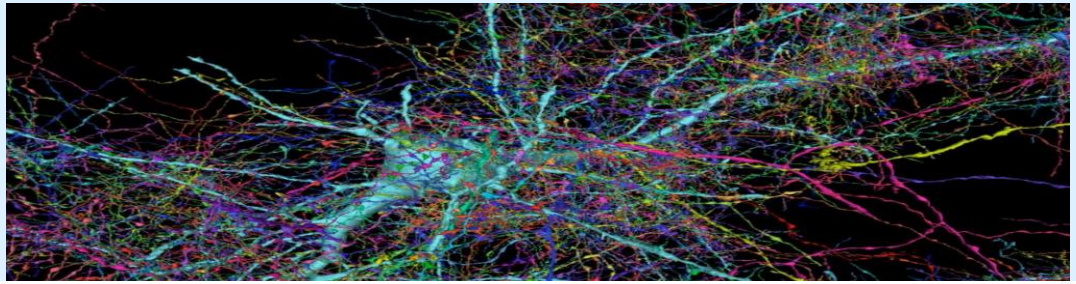
Deep Learning

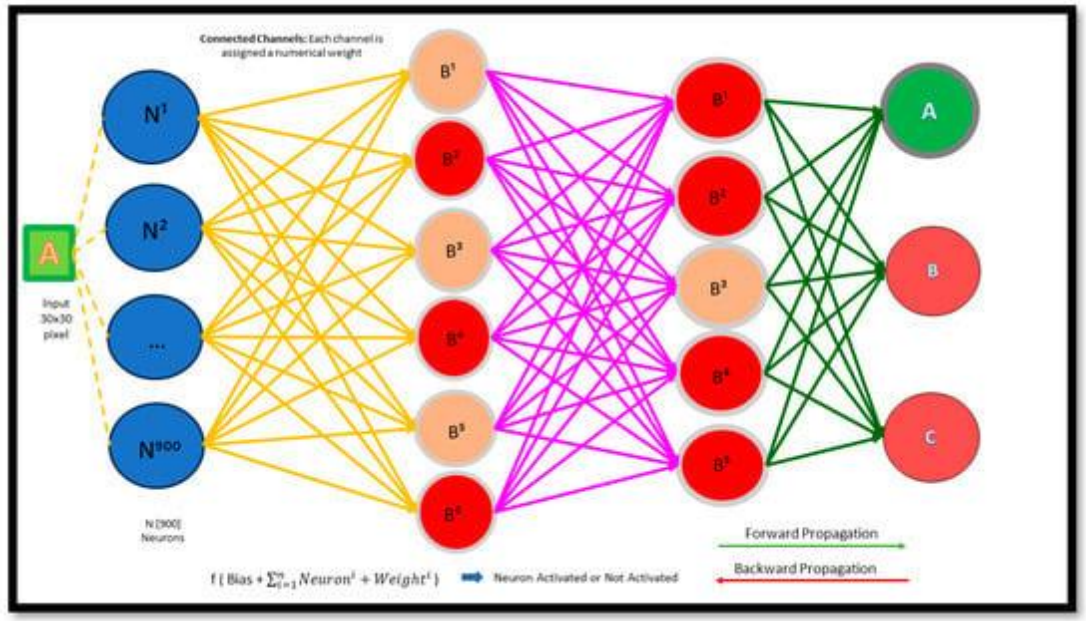
Sottoinsieme del Machine Learning che utilizza dati non strutturati, senza pre-elaborazione, tipicamente usando Reti Neurali Artificiali (ANN)

DEEP LEARNING

Modello di apprendimento automatico (USML)

- Usa grandi quantità di dati per addestramento e predizione
- Richiede potenza di calcolo di alto livello; sono necessarie GPU
- Richiede molto tempo per l'addestramento del modello
- Utilizza complessi modelli non lineari di correlazione
- Output è solitamente espresso in vari formati, non solo numerici





NEURAL NETWORK

Strutture SW e/o HW ispirate al cervello umano

Comprendono più strati:

- Tra i livelli di input e di output si trovano diversi livelli nascosti (anche centinaia o migliaia)
- Ogni livello nascosto prende l'input dal livello precedente, esegue alcuni calcoli e passa l'output al livello successivo
- Questo processo continua, anche bidirezionalmente, fino a quando l'output non viene inviato al layer di output, che fornisce il risultato finale o la previsione.

Applicazioni tipiche dell'Intelligenza Artificiale (non esaustivo)

Intelligent Data Processing

algoritmi che analizzano dati specifici per estrapolare informazioni e compiere azioni in conseguenza del risultato (analisi predittiva, rilevamento frodi)

Virtual Assistant/Chatbot

agenti software in grado di eseguire azioni o erogare servizi per un individuo in base a comandi ricevuti in maniera vocale o testuale (customer care aziendale, assistenza di primo livello)

Recommendation System

indirizzo scelte utenti in base ad informazioni da essi fornite in maniera diretta o indiretta (suggerimento in base a precedenti acquisti, customer journey o altre forme di profilazione)

Natural Language Processing

Soluzioni che elaborano il linguaggio, con finalità che possono variare dalla comprensione del contenuto, alla traduzione, fino alla produzione di testo in modo autonomo a partire da dati o documenti forniti in input.

Computer Vision

comprensione di alto livello del contenuto di immagini o video, orientate al riconoscimento di persone, animali e cose presenti all'interno dell'immagine stessa, riconoscimento biometrico e in generale all'estrazione di informazioni dall'immagine.

Soluzioni fisiche

oggetti in grado di compiere azioni senza l'intervento umano e di prendere decisioni in base a informazioni raccolte dall'ambiente circostante (Autonomous Vehicle, Autonoumos Robot, …)

source: Politecnico di Milano

La novità: Intelligenza Artificiale Generativa (Gen-AI)

Modello di Machine Learning in grado di generare nuovi dati invece di generare previsioni, raccomandazioni, decisioni



Come suggerisce il nome, l'IA generativa è in grado di generare nuovi contenuti - tra cui testo, immagini, audio, codice, simulazioni e video – mentre interpreta e manipola dati preesistenti

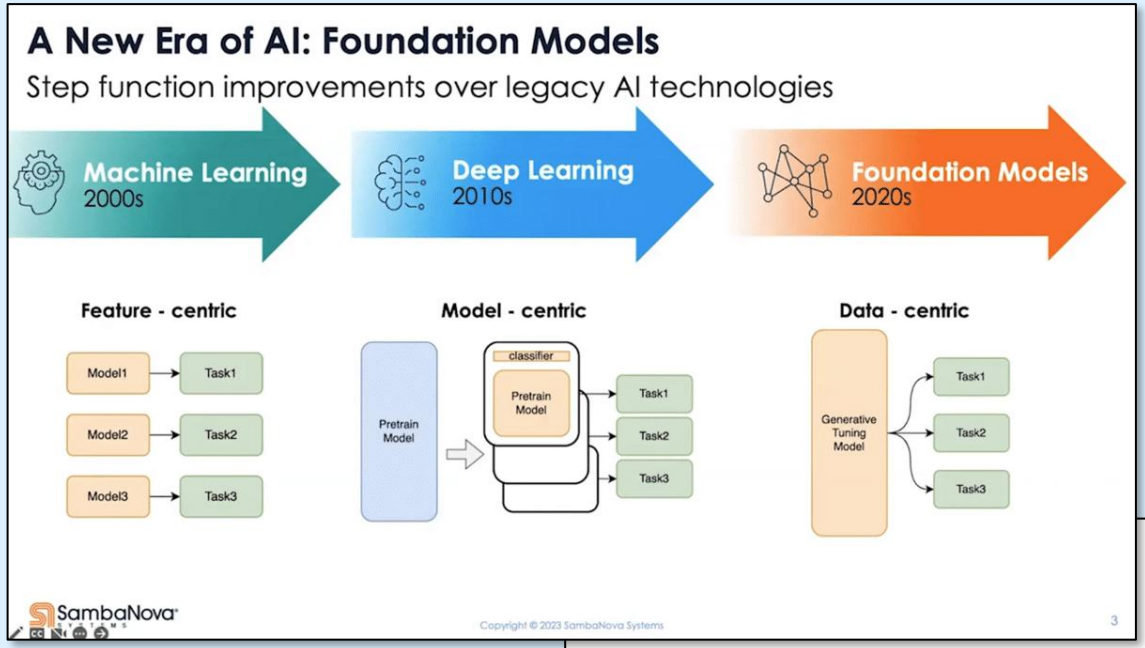
Modality	Application
Text	Content writing Chatbots or assistants Search Analysis and synthesis
Code	Code generation Application prototype and design Data set generation
Image	Stock image generator Image editor
Audio	Text to voice generation Sound creation Audio editing
3-D or other	3-D object generation Product design and discovery
Video	Video creation Video editing Voice translation and adjustments Face swaps and adjustments

Mc Kinsey, What's the future of generative AI?, August 2023

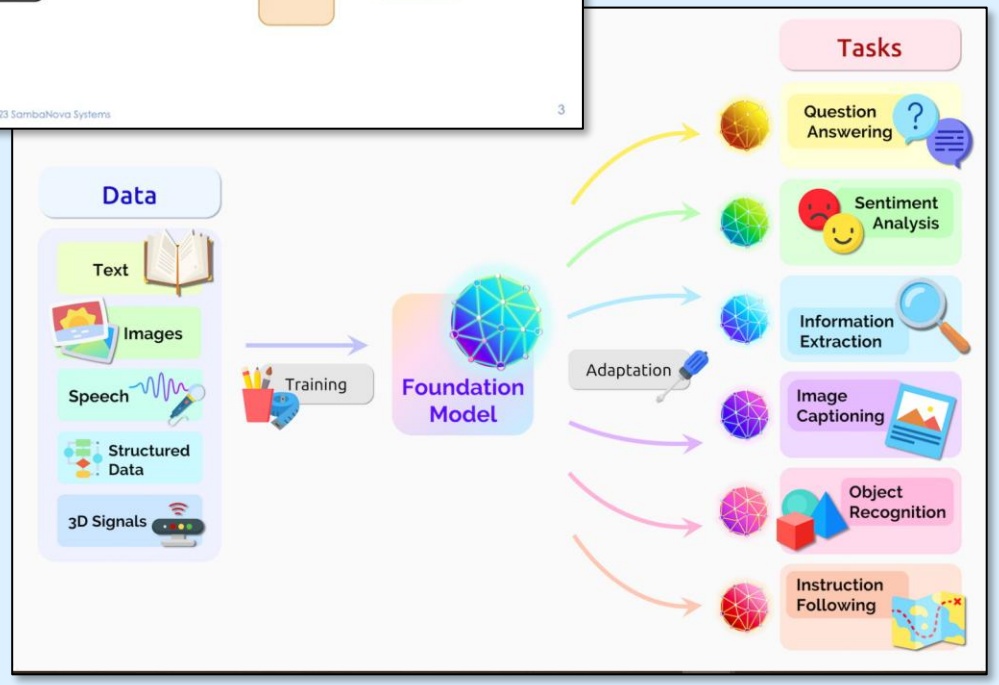
Gen-AI: una novità?

- *IA generativa non è un concetto nuovo: sono le tecniche di apprendimento automatico alla base dell'IA generativa ad essersi evolute nell'ultimo decennio*
- *Combinando l'apprendimento non supervisionato con l'architettura di rete neurale chiamata "transformer", sono emersi i cosiddetti "foundation models", modelli di base di grandi dimensioni in grado di gestire più modalità di dati*
- *Fungono da punto di partenza per lo sviluppo di modelli più avanzati e complessi. Si possono creare modelli specializzati e più sofisticati su misura per casi d'uso o domini specifici.*

IBM, What is generative AI, what are foundation models, and why do they matter?, March 2023



Snorkel team, Practical solutions: enterprise value from foundation models, March 2023



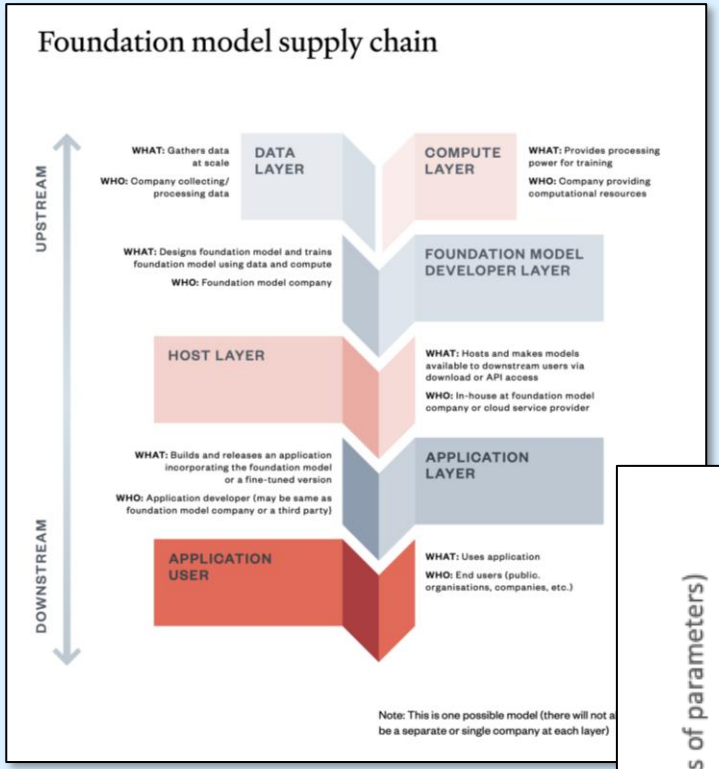
R. Merritt Nvidia, What are foundation models ?, March 2023

Gen-AI: Supply Chain e trend potenzialità

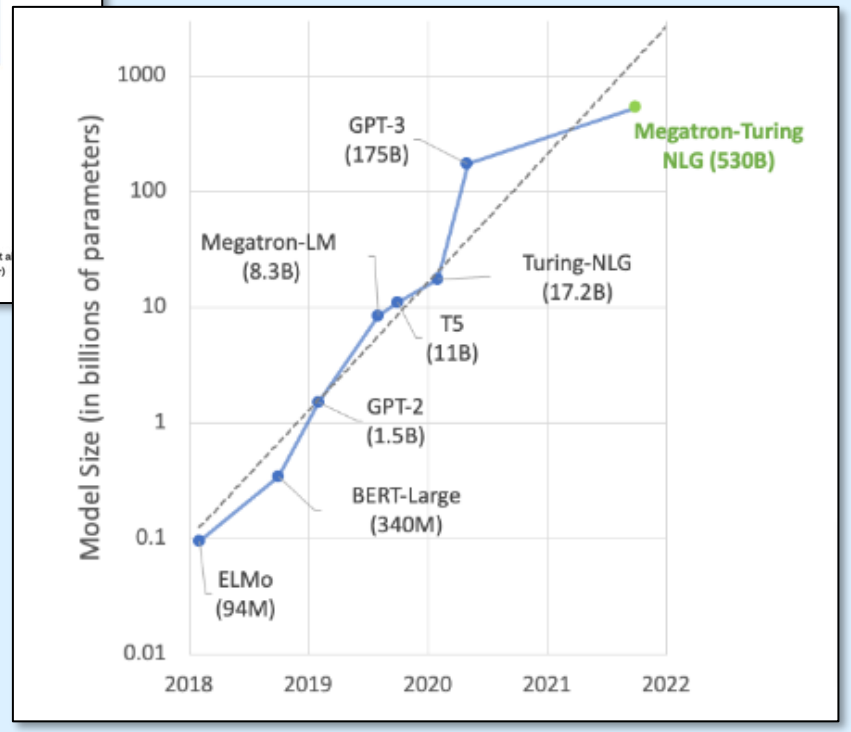
- *La Supply Chain della Gen AI è strutturata su più livelli / attori*
  - *Raccolta ed elaborazione dati su larga scala - Fornitura risorse computazionali per l'addestramento*
  - *Sviluppo modello di base (FM)*
  - *Hosting e messa a disposizione del modello (API)*
  - *Sviluppo applicazioni incorporanti il modello o fine tuning*
  - *Uso applicazioni (end users)*

- *Aumento capacità sistemi Gen-AI (parametri modello)*

2018	*100 milioni*	*(10^8)*
2019	*1 miliardo*	*(10^9)*
2020	*11 miliardi*	*(10^{10})*
2021	*175 miliardi*	*(10^{11})*
2022	*1 trilione*	*(10^{12})*
oggi	*>10 trilioni*	*(10^{14} ?)*



Ada Lovelace Institute, Explainer: What is a foundation model?, July 2023



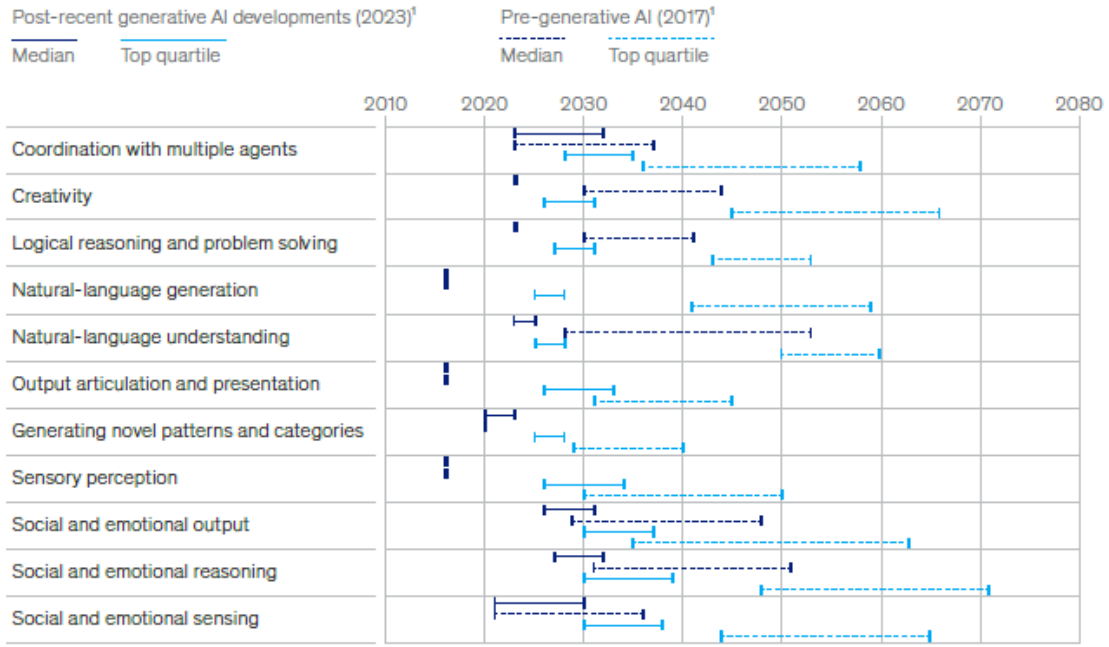
Neuroflash, Parametri GPT-4 – voci e previsioni, Feb 2023

Il vero elemento di “novità”

“The road just got shorter: automation of knowledge work is now in sight”

“Technology could achieve human-level performance sooner than previously thought”

Estimated range for technology to achieve human-level performance, by technical capability

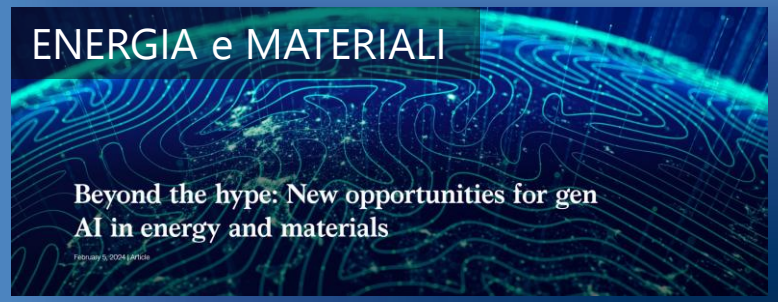


[1]Comparison made on the business-related tasks required from human workers.
Source: McKinsey Global Institute occupation database; McKinsey analysis

McKinsey & Company
(What’s the future of generative AI?, August 2023)

“Gen AI represents just a small piece of the value potential from AI”

Gen-AI: un mercato orizzontale che abbraccia tutti i mercati verticali



















McKinsey & Company, Generative AI: Industry perspectives, March 2024

Gen-AI nelle aziende, in pratica …

Miglioramento ricerca e innovazione

Possibilità di riassumere i contenuti, delineare più percorsi per raggiungere una soluzione, fare brainstorming e creare documentazione dettagliata a partire da note di ricerca
(ad esempio, i sistemi di IA generativa vengono utilizzati nell'industria farmaceutica per generare e ottimizzare sequenze proteiche e accelerare in modo significativo la ricerca sui nuovi farmaci)

Miglioramento esperienza dei clienti

Può fungere da strumento per il servizio clienti e la personalizzazione dei flussi di lavoro dei clienti
(ad esempio, è possibile utilizzare chatbot, bot vocali e assistenti virtuali che rispondono in modo più accurato ai clienti per la risoluzione del primo contatto. Possono migliorare il coinvolgimento dei clienti proponendo offerte e comunicazioni selezionate in modo personalizzato)

Ottimizzazione processi aziendali

È possibile applicare questa tecnologia a tutte le linee di impresa, tra cui ingegneria, marketing, assistenza clienti, finanza e vendite
(ad esempio, estrarre e riassumere i dati da qualsiasi fonte per le funzioni di ricerca di informazioni: valutare e ottimizzare diversi scenari per la riduzione dei costi in aree come marketing, pubblicità, finanza e logistica: generare dati sintetici per creare dati etichettati per l'apprendimento supervisionato e altri processi di machine learning)

Miglioramento produttività dei dipendenti

I modelli possono migliorare i flussi di lavoro dei dipendenti e fungere da assistenti efficienti per l'intero personale aziendale
(ad esempio, supportare le attività creative generando più prototipi basati su determinati input e vincoli, ottimizzare i progetti esistenti sulla base del feedback umano e di vincoli specifici, generare nuovi suggerimenti di codice software per le attività di sviluppo di applicazioni, supportare la gestione generando report, riassunti e proiezioni, generare nuovi script di vendita, contenuti per le e-mail e blog per i team di marketing)

Rischi potenziali della Gen-AI

Accuratezza

I modelli di Gen-AI possono "inventare" risposte che sembrano credibili (a volte indicate come "allucinazioni") o possono avere un ragionamento astratto scadente. Le risposte che potrebbero sembrare di alta qualità possono in realtà essere di scarso valore per gli utenti finali

Etica

Come l'IA tradizionale, la Gen-AI a volte può produrre output distorti, usabili strumentalmente. Può anche essere utilizzato in modo improprio per aggirare le misure di sicurezza

Privacy

I dati sensibili o riservati possono essere divulgati tramite API LLM pubbliche. Necessario suddividere i dati a disposizione degli LLM per allineare i controlli di accesso già esistenti

Sicurezza

La Gen-AI è suscettibile agli attacchi backdoor, che a volte possono passare inosservati. Ci sono già stati casi di hacker che hanno creato disinformazione, rubato dati o commesso frodi

Legali

Esistono rischi di violazione della proprietà intellettuale e del copyright, e di responsabilità per uso improprio. Il modo in cui le leggi si applicano agli output creati dalla generazione dell'IA è ancora ambiguo

McKinsey & Company, Generative AI: Industry perspectives, March 2024

Eppur si muove …

Via libera del Parlamento Ue all'AI Act: cosa prevede la prima legge al mondo sull'intelligenza artificiale

13 MARZO 2024 - 13:51



Con sufficienti chiarezza, efficacia e velocità?

Crescita inclusiva, sviluppo sostenibile e benessere

focalizza le potenzialità positive dei sistemi affidabili di IA, al fine di realizzare gli obiettivi generali di sviluppo globale sostenibile da cui dipende la crescita complessiva della società, come priorità di intervento preordinata al perseguimento del bene comune, superando le diseguaglianze tecnologiche esistenti

Valori centrati sulla persona ed equità

la progettazione dei sistemi di IA, durante l'integrale ciclo di vita, deve sempre avvenire nel rispetto dei diritti umani e dei valori democratici mediante il riconoscimento di adeguate garanzie per realizzare una società giusta ed equa

Trasparenza e spiegabilità

stabilisce il diritto degli utenti di conoscere pienamente le modalità di funzionamento dei sistemi di IA nell'ambito di una divulgazione responsabile in grado di fornire informazioni complete, significative e coerenti con lo stato dell'arte esistente

.Robustezza, sicurezza e protezione

necessità di assicurare, mediante una costante supervisione umana, periodici monitoraggi di controllo sul funzionamento sicuro e protetto dei sistemi di IA, garantendo la tracciabilità dei risultati al fine di prevenire il rischio di usi impropri illeciti e dannosi.

Responsabilità

afferma l'esistenza di un generale regime di responsabilità a carico delle persone (fisiche e giuridiche) che "sviluppano, implementano o gestiscono sistemi di IA" nei casi di accertati pregiudizi cagionati in violazione dei principi richiamati.

Principi e orientamenti enunciati dall'OCSE

E noi? (a cosa prestare attenzione)

- L'intelligenza artificiale avrà un impatto su ogni campo, che si tratti di arte e discipline umanistiche, scienze sociali, scienze mediche o ingegneria …
  - … solo per citarne alcuni: le aziende e le istituzioni devono investire in strumenti e talenti per rimanere al passo
- Anche l'IA generativa va considerata come uno strumento per supportare gli esseri umani, non come uno strumento per sostituire gli esseri umani
  - Il ruolo della governance dei dati all'interno di un'organizzazione è diventato ancora più critico (serve quadro chiaro e attuabile di utilizzo Gen-AI, protocolli adeguati per evitare di esporre la loro proprietà intellettuale).
  - Vanno rivalutate le linee guida relative a imbrogli e plagio.
  - Servono più controlli ed equilibri nello sviluppo e l'utilizzo delle applicazioni (la scrittura di un programma autonomo differisce in modo significativo da un'applicazione aziendale che potrebbe interfacciarsi con altri sistemi …).
- Gli strumenti associati all'IA sono qui per restare, e dobbiamo noi (tutti) imparare a gestirli
  - Essenziale la formazione continua sulla natura e l'impatto dell'IA nei vari e rispettivi campi …

