

AI e Altre Tecnologie emergenti. Rischio o opportunità?

NUOVE SFIDE, OPPORTUNITÀ E RISCHI DA AI E ALTRE TECNOLOGIE IT.

COSA FARE?



Il Dubbio: Rischio o opportunità?



Cosa si è fatto e cosa si può fare



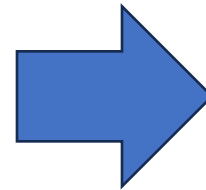
L'AI che vorrei

Il dubbio sulle tecnologie emergenti e su AI



Opportunità

Sistemi per migliorare il Lavoro, velocizzare operazioni, aumentare tempo libero, migliorare la propria vita, renderci autonomi e più potenti



o rischio?

Rischio di perdere il controllo, perdere il contatto con la realtà, diventare Schiavi delle stesse tecnologie o delle aziende che governano la tecnologia

Stiamo vivendo un'epoca di straordinaria trasformazione

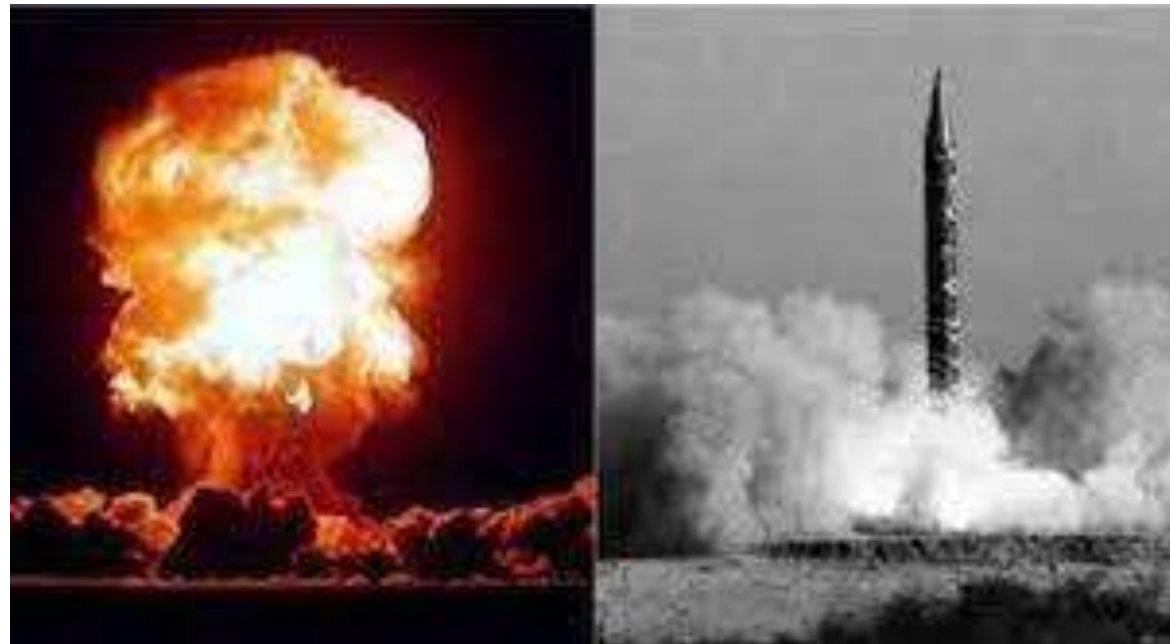


E' l'alba di un nuovo giorno o l'inizio del declino dell'Uomo?

Rischi nell'utilizzo dell'AI

Laura Nolan (ex ricercatrice di Google) ha affermato di recente, con un'intervista al "The Guardian" che l'IA potrebbe avviare guerre o commettere atrocità di massa. "Pochissime persone ne parlano, ma se non stiamo attenti, **robot assassini potrebbero accidentalmente iniziare una guerra lampo**, distruggere una centrale nucleare e causare atrocità di massa".

Rischio



Eugeniy Morozov (Prof. Stanford University)

Opportunità



«La libertà di scelta, semplicemente non esiste più. Algoritmi sempre più sofisticati potevano tracciare rapidamente l'identikit degli utenti, offrendo contenuti "mirati" rispetto alle preferenze espresse da costoro, più o meno consapevolmente, nel corso di precedenti ricerche online. Poco più tardi, il perfezionamento delle funzioni predittive degli algoritmi che governano i motori di ricerca avrebbe generato un ulteriore paradosso: **informazioni offerte agli utenti prima ancora che costoro potessero formulare una preferenza.**»

Rischio

Progressiva esternalizzazione delle funzioni umane



Memoria



Calcolo



Intelligenza



Responsabilità



Identità



Percezione e estensione dei 5 sensi



Cognizione di se: io non sono più quello che sono ma quello che appaio sui social



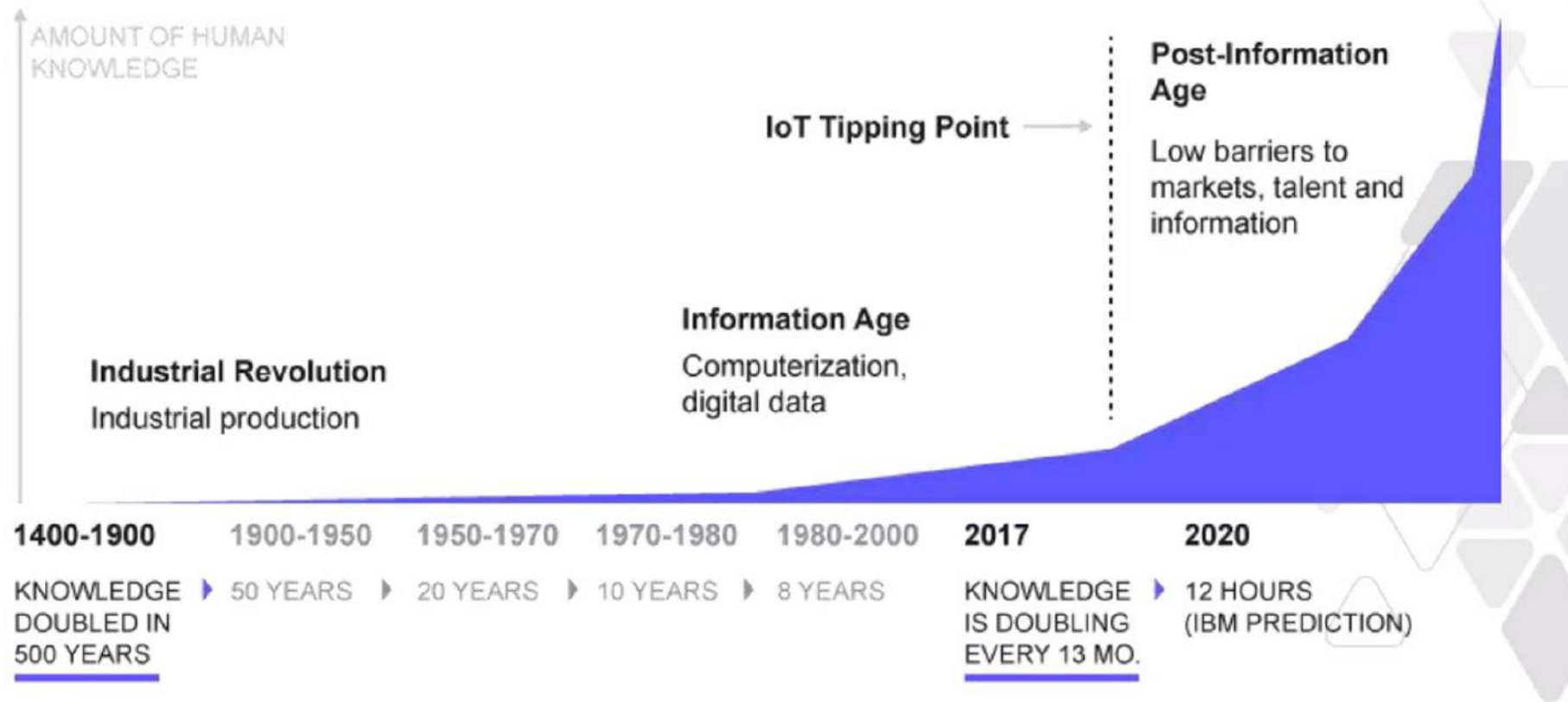
Coscienza?

Opportunità

Rischio

Perchè si usa AI

L'esplosione della conoscenza



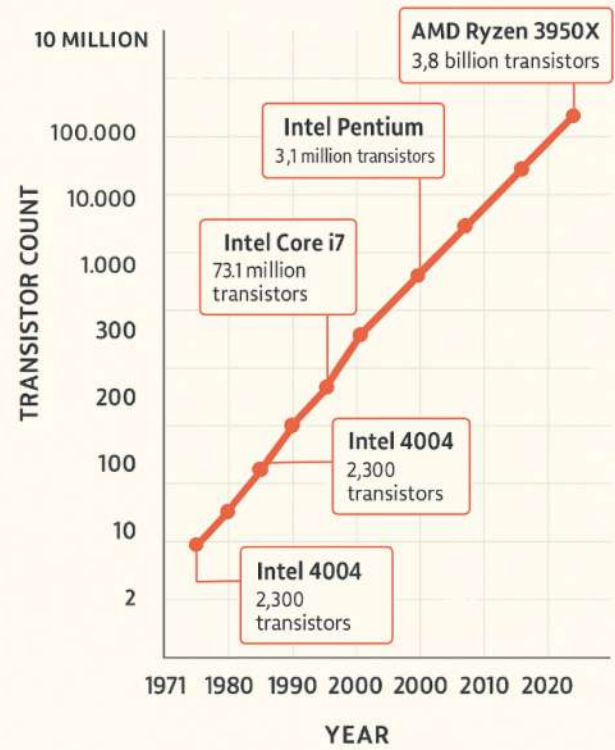
Capacità di governare la massa di informazioni e di conoscenza

Conseguenze della evoluzione delle nuove tecnologie

Opportunità

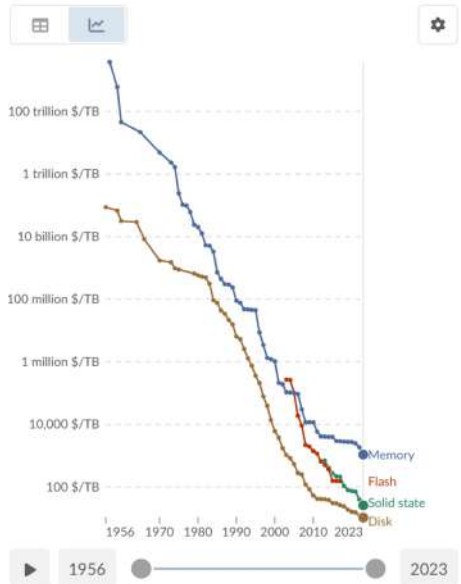
MOORE'S LAW

The number of transistors on a microchip doubles approximately every two years.



Historical price of computer memory and storage

This data is expressed in US dollars per terabyte (TB), adjusted for inflation. "Memory" refers to random access memory (RAM), "disk" to magnetic storage, "flash" to special memory used for rapid data access and rewriting, and "solid state" to solid-state drives (SSDs).

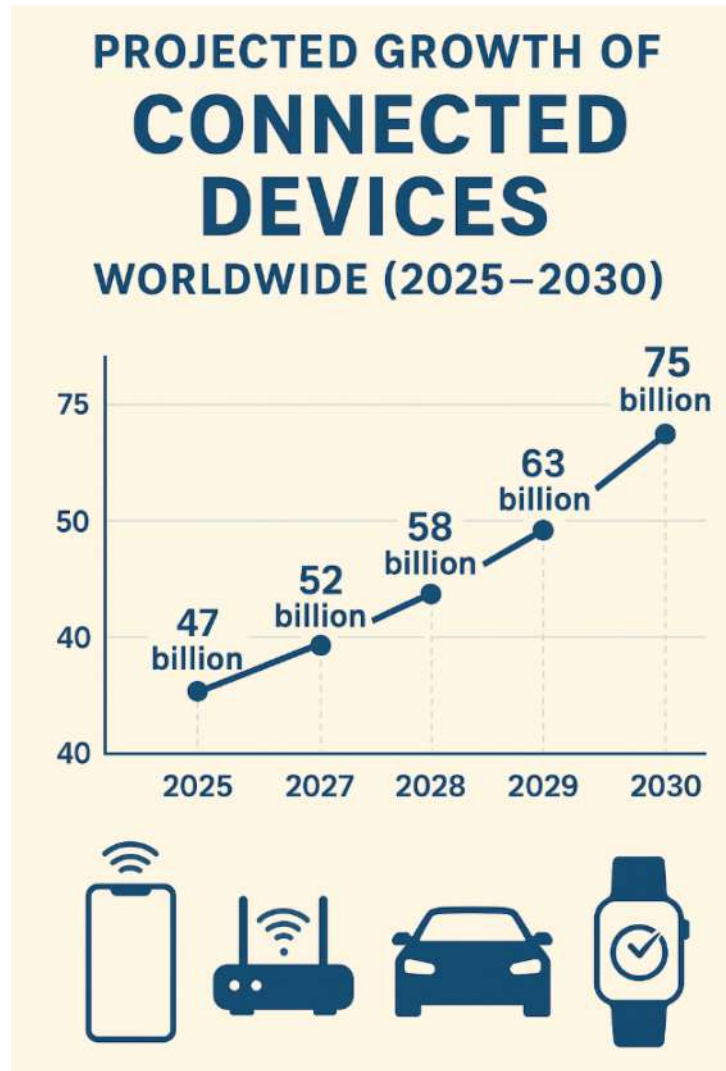


Data source: John C. McCallum (2023); U.S. Bureau of Labor Statistics (2024) - [Learn more about this data](#)
Note: For each year, the time series shows the cheapest historical price
2023
in constant 2020 US\$ per terabyte

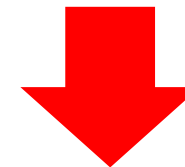
Category	Price (\$/TB)
Memory	1,088
Solid state	26
Disk	11



Crescita dei dispositivi connessi IOT



Il numero di dispositivi connessi per persona cresce dallo 0,08 nel 2003 al 1,1 nel 2010 a circa 4 nel 2017 a circa 8 nel 2025



Grande Quantità di Dati

Zettabyte

WHAT'S A ZETTABYTE?

1 kilobyte	1,000	000,000,000,000,000,000
1 megabyte	1,000,000	000,000,000,000,000
1 gigabyte	1,000,000,000	000,000,000,000
1 terabyte	1,000,000,000,000	000,000,000
1 petabyte	1,000,000,000,000,000	000,000
1 exabyte	1,000,000,000,000,000,000	000
1 zettabyte	1,000,000,000,000,000,000,000	

- Uno studio della Berkeley ha stimato che **dall'inizio dell'umanità fino alla diffusione del computer (1980)** l'umanità ha accumulato 12 exabyte di dati
- **Dal 1980 al 2006** ha accumulato altri 180 exabyte
- **Dal 2006 al 2011** la stima è di 1,6 zettabyte
- **Dal 2011 al 2024** la stima è di 147 zettabyte
- **Nei prossimi 10 anni:** Non solo il volume dei dati ma anche la stessa velocità di accumulo si stima che continueranno a crescere

Un potere di computazione sempre più grande a disposizione di un sempre maggior numero di persone in una quantità e velocità mai viste.

Dove ci porta questo fenomeno?

1-Marea Informativa

Rischio

Nessuno ci costringe a digerire ogni bit disponibile ma ...



quando l'insieme di dati è talmente grande e complesso da renderne difficile il processamento utilizzando strumenti tradizionali si può ricorrere ad algoritmi o all'AI

Demandare potenza intellettuale: AI Analytics



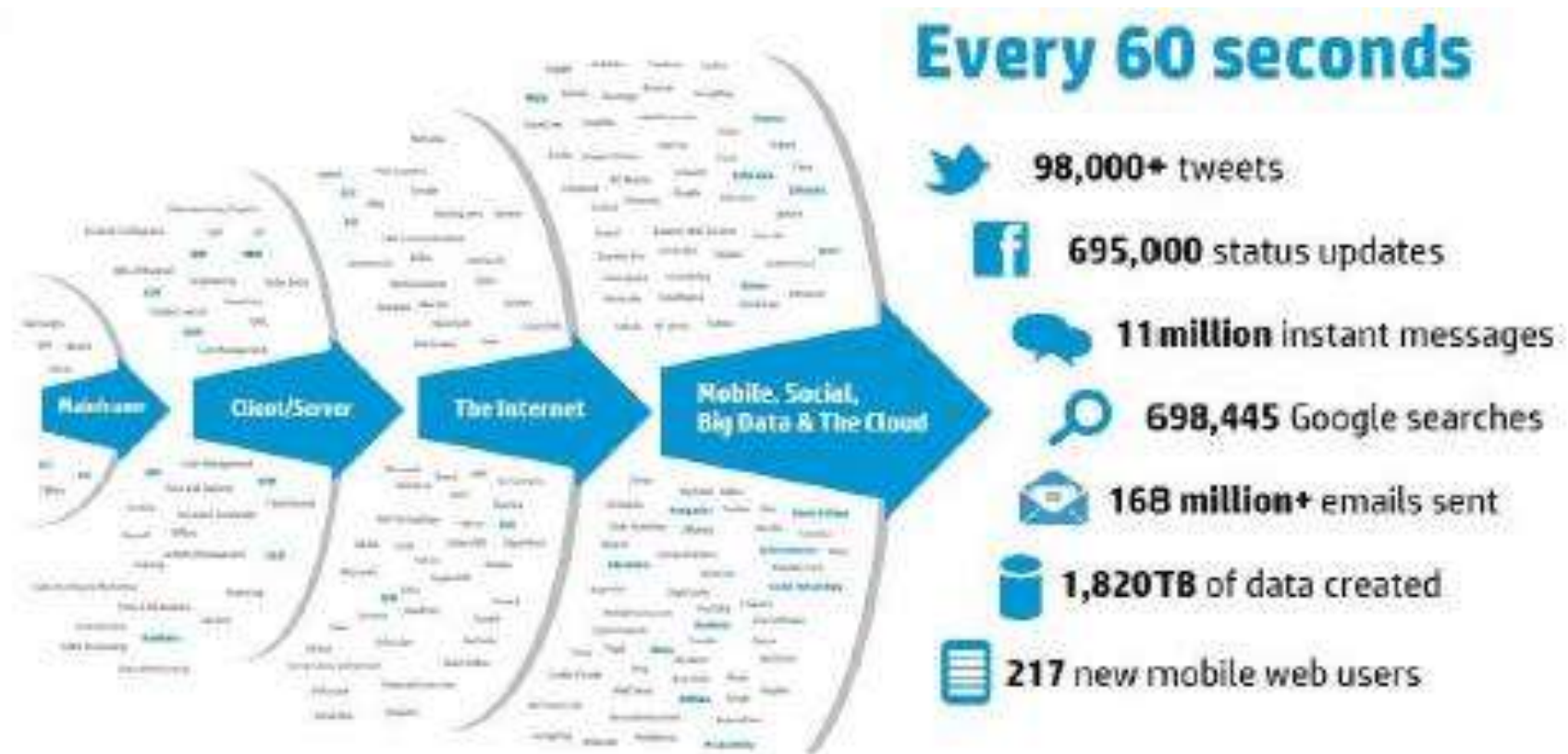
Opportunità

Individuare dove reperire, in immensi database, nuovi pattern e come sfruttare queste relazioni per creare intelligenza e valore aggiunto.

Rischio

Chi riesce a sfruttare modelli di analisi meglio o più velocemente di noi, verrà assunto al posto nostro, costringerà la nostra azienda a uscire dal mercato, ci farà mancare una scoperta o un nobel.

News



Nel 2007 il mondo ha prodotto più dati di quanti ne possa immagazzinare

2 -Rischio: Oblivio colposo



Quando il governo della cancellazione dei dati è nostro possiamo inventarci un algoritmo più o meno conservativo.

Sempre più spesso invece il governo della cancellazione dei dati negli spazi cloud è demandato ad un algoritmo AI.

C'è un rischio concreto che dati importanti non utilizzati continuamente finiscano «dimenticati» definitivamente.

Siamo nelle mani di ...

Rischio



OpenAI



Meta AI

aws



E se ci spengono questo bocchettone.

Quantum computing



Opportunità

Grandi opportunità per fattorizzazione di grandi numeri, per le simulazioni di molecole, per la crittografia

Rischio

Mette a rischio gli attuali sistemi di crittografia, Concentrazione della capacità di ricerca e di innovazione nelle mani di sempre meno centri nel mondo

3-Rischi sistemici per l'EU



Mancanza di infrastrutture digitali europee
Scarso capitale a rischio per stare nel mercato mondiale

Eurovision song contest 2025 - Promo

<https://www.youtube.com/watch?v=VaJQaK73vF4+ù>



FRODE: Obiettivo conquistare la fiducia della potenziale vittima

Phishing

Mail generate da
intelligenza digitale

Frodi a cottura lenta.

deep fake

si clona la voce o
addirittura si creano dei
falsi avatar molto simili
all'originale.

Volume di affari delle
frodi paragonabile a
quello della droga.
Raddoppiato dal 2023

82% delle transazioni
fraudolente effettive sono
operate da cliente stesso
(fonte Certfin)

La Perdita di fiducia è il
rischio più importante per
l'AI e le nuove tecnologie

4-FRODE Minaccia la fiducia



L'AI favorisce nella cybersecurity gli attaccanti e **mina al cuore del rapporto fiduciario** che c'è tra cliente e banca, tra utente e sistemi, tra consumatore e cliente, tra Azienda e Azienda, tra PA e Cittadino. Minaccia la credibilità delle istituzioni, la sicurezza fisica dei cittadini.

La fiducia è la vera infrastruttura da difendere e su cui investire.

Esempi di Rischi aziendali “operativi”



Sicurezza del software.

OWASP, scrittura automatica di software, test automatici, scrittura di Software effimeri o temporanei



Allucinazioni

L'AI è studiata per dare sempre una risposta anche se non è necessariamente quella giusta o vera

Allucinazioni nel campo delle risposte relative ai propri investimenti o alla consistenza dei conti non sono ammessi.



BIAS

Modelli addestrati su informazioni che prevedono pregiudizi di razza, genere o orientamenti sessuali

Esempio modelli di rating



Catena fornitori

Valutazione se nella catena dei fornitori dei nostri servizi tutti i sottocomponenti sono «certificati» secondo gli standard che ci vogliamo dare

La sfida dei modelli AI

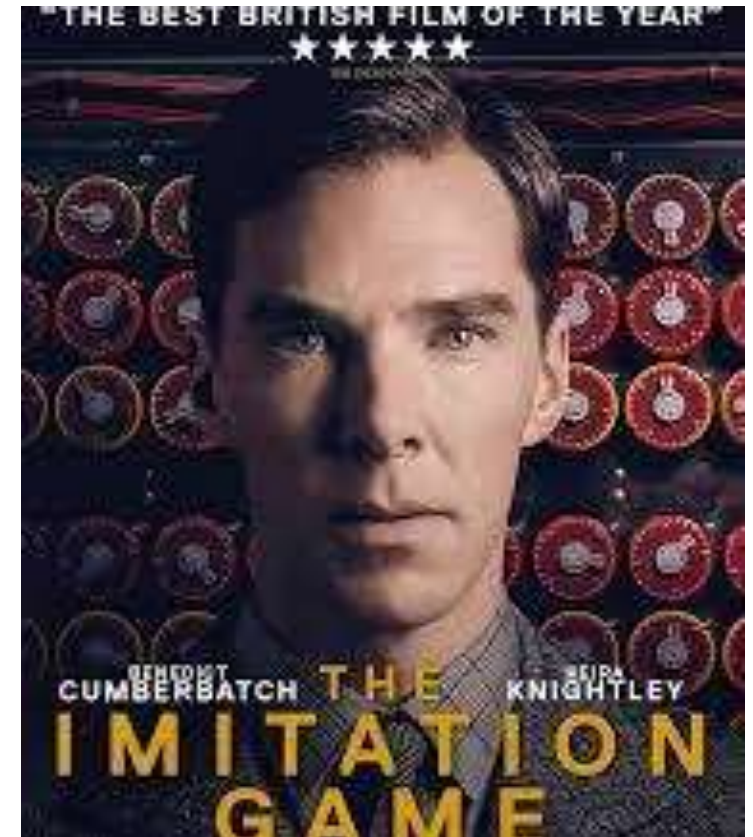
Gestione dinamica dei goal, risoluzione dei conflitti tra goal differenti, ragionamento, adattamento al contesto, allineamento dei valori sottostanti ai goal, aggiornamento continuo degli obiettivi:

Alziamo l'asticella della sfida del ragionamento dall'intelligenza alla coscienza.

Test di Touring

«ci sarà un momento in cui capiamo che la macchina ha raggiunto un livello di evoluzione simile all'uomo e sarà quando non riusciremo a distinguere più in una conversazione se siamo di fronte ad un uomo o ad una macchina.»

Il prossimo test di Touring fa un po' paura ed è un test in cui la macchina si mette da parte e incomincia ad individuare ed elaborare un concetto di coscienza autonomo, senza che nessuno lo abbia suggerito o detto.



Cosa si è fatto e cosa si può fare



Principi fondanti dell'Unione Europea che derivano dai trattati di Roma dopo solo 12 anni dalla fine della Seconda Guerra Mondiale

La dignità umana è inviolabile. Difesa della democrazia, Perseguire l'uguaglianza dei diritti, Difendere i Diritti Umani

L'impatto delle nuove tecnologie nell'agenda dell'UE



AI Act ha una visione umanocentrica che ci costa ma porta ad un AI responsabile

Artificial Intelligence Act

Cosa è

AI (acronimo di Artificial Intelligence) Act è un Regolamento europeo che ha l'obiettivo di promuovere un'IA **antropocentrica** e **affidabile**. Stabilisce regole armonizzate per l'immissione sul mercato e l'uso di sistemi di IA, proibizioni per determinate pratiche di IA, requisiti per i sistemi di IA ad alto rischio, obblighi per gli operatori di tali sistemi e misure di trasparenza.

1. Governance

Organi di gestione del AI Act

2. Rischio AI

AI vietate e ad alto rischio

3. AI Finalità generali

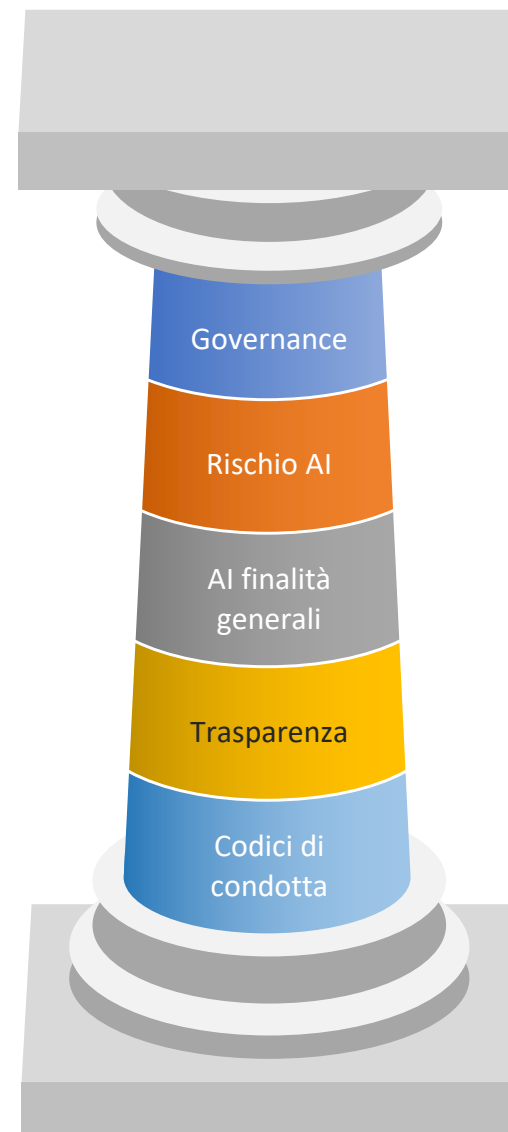
Modelli IA con finalità generali

4. Trasparenza

Fornitori e deployer

5. Codici di condotta

Best practices in ambito AI



Soluzioni Augeos per la governance dei rischi

Augeos offre **soluzioni software, consulenza e formazione** con un focus sul mondo finance ma non solo. Offriamo soluzioni personalizzate per affrontare le sfide legate a **EU AI Act, DORA, GDPR, rischi operativi, IT Risk Management, esternalizzazione di funzioni di controllo.**

01

Consulenza

La nostra offerta di consulenza Augeos Advisor si concentra sulla progettazione e implementazione di percorsi di conformità DORA, GDPR, EU AI Act.

02

Formazione

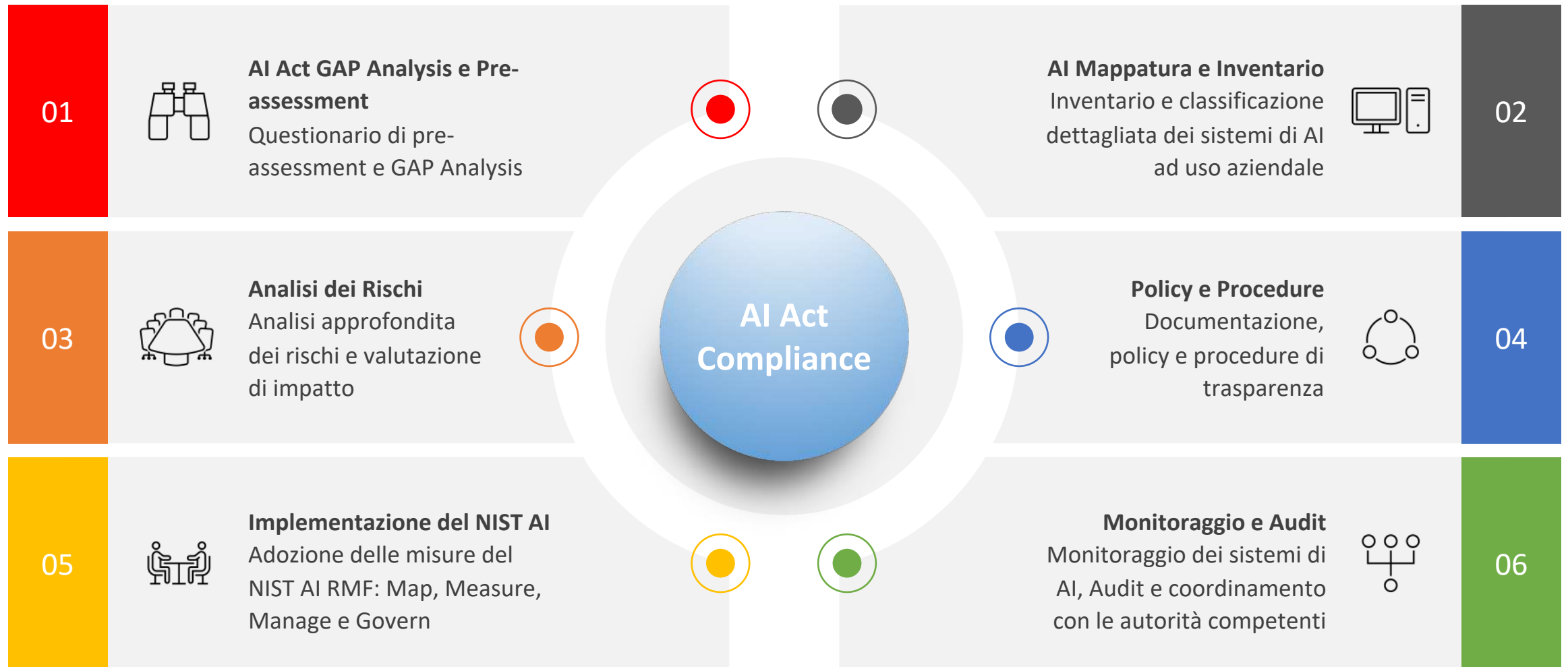
La formazione del personale è fondamentale per affrontare le sfide inerenti DORA, GDPR, AI, protezione dei dati e cybersecurity.

03

Supporto Tecnologico

Il supporto tecnologico offerto attraverso GRC4 garantisce strumenti di governance dei rischi per la conformità normativa delle aziende.

Advisor Consulenza AI Act



AI Act Risk-based approach - Piramide del rischio



AI Act spiegato dalla Commissione Europea

- ❑ **Intelligenza Artificiale:** che cos'è e quali sono le tecnologie di Intelligenza Artificiale generativa in ambito finance soggette al AI Act
- ❑ **AI Act:** definizioni introduttive e ambito di applicazione
- ❑ Che cosa si intende per **alfabetizzazione** IA e cosa comporta
- ❑ Le **sanzioni** che si rischiano in caso di mancato rispetto del Regolamento
- ❑ Gli organismi di Governance a livello dell'Unione



Introduzione al AI Act in ambito finance

Panoramica del
Regolamento
sull'Intelligenza
Artificiale e sulle
tecnologie AI

- ❑ La **piramide** del rischio AI
- ❑ Rischio inaccettabile e pratiche **AI vietate**
- ❑ **Rischio alto** e obblighi di compliance per gli operatori nel settore finance
- ❑ I requisiti di conformità per **fornitori** e **deployer**
- ❑ I modelli di intelligenza artificiale general purpose e a **rischio sistemico**
- ❑ Il **NIST AI** Risk Management Framework
- ❑ **Mitigazione** del rischio AI

2

AI Act e Governance del Rischio

Gestione e
mitigazione dei
rischi legati
all'introduzione
dell'Intelligenza
Artificiale

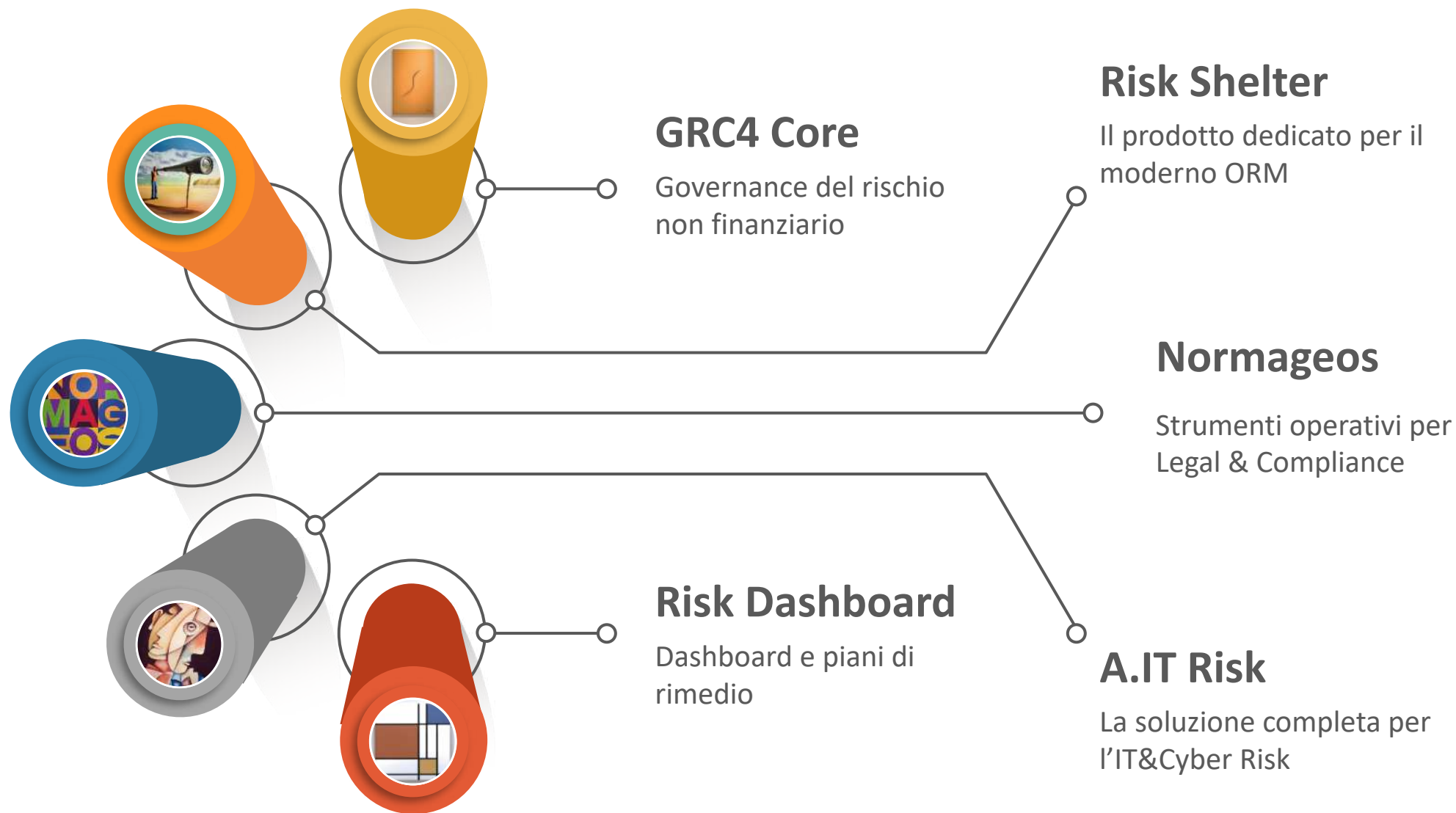
- ☐ I punti di intersezione tra **privacy** e **AI Act**
- ☐ Gli **scenari di rischio** legati all'utilizzo di AI Generativa come ChatGPT
- ☐ **AI Policy** nel settore finance
- ☐ I requisiti di **trasparenza**
- ☐ I codici di **Condotta**
- ☐ Le **Hallucinations** e casi di studio in ambito finance
- ☐ **Q&A conclusiva** a chiusura del percorso formativo

3

Questioni etiche e Privacy

Implicazioni etiche
legate a bias,
discriminazioni e
utilizzo dei dati
personali senza
opportuno consenso

GRC4: Innovazione e Tradizione al servizio della governance dei rischi



L'AI che vorrei



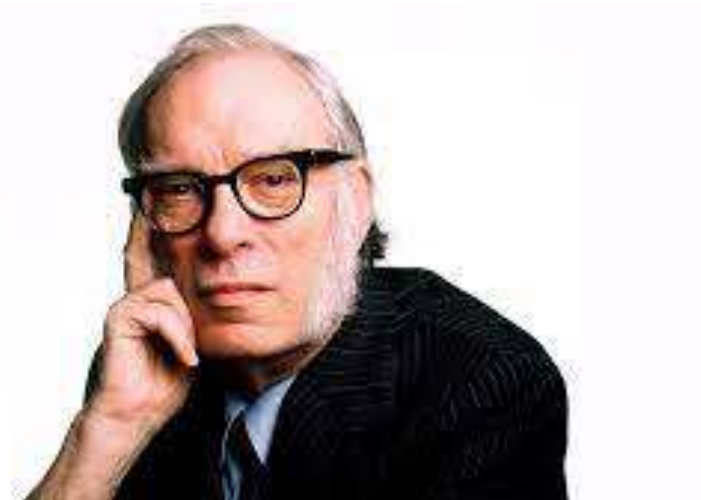
I have a dream...

Inserire regole etiche negli algoritmi

LE TRE LEGGI DELLA ROBOTICA

1. Un robot non può recar danno a un essere umano né può permettere che, a causa del suo mancato intervento, un essere umano riceva danno.
2. Un robot deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non vadano in contrasto alla Prima Legge.
3. Un robot deve proteggere la propria esistenza, purché la salvaguardia di essa non contrasti con la Prima o con la Seconda Legge.»

(Manuale di Robotica, 56ª Edizione - 2058 d.C.)



La sfida della trasparenza



Spiegare le scelte effettuate da algoritmi di AI

Al senza pregiudizi



AI Rispettosa della Privacy



Al Rispettosa dei diritti d'autore



Al Rispettosa della sicurezza nazionale



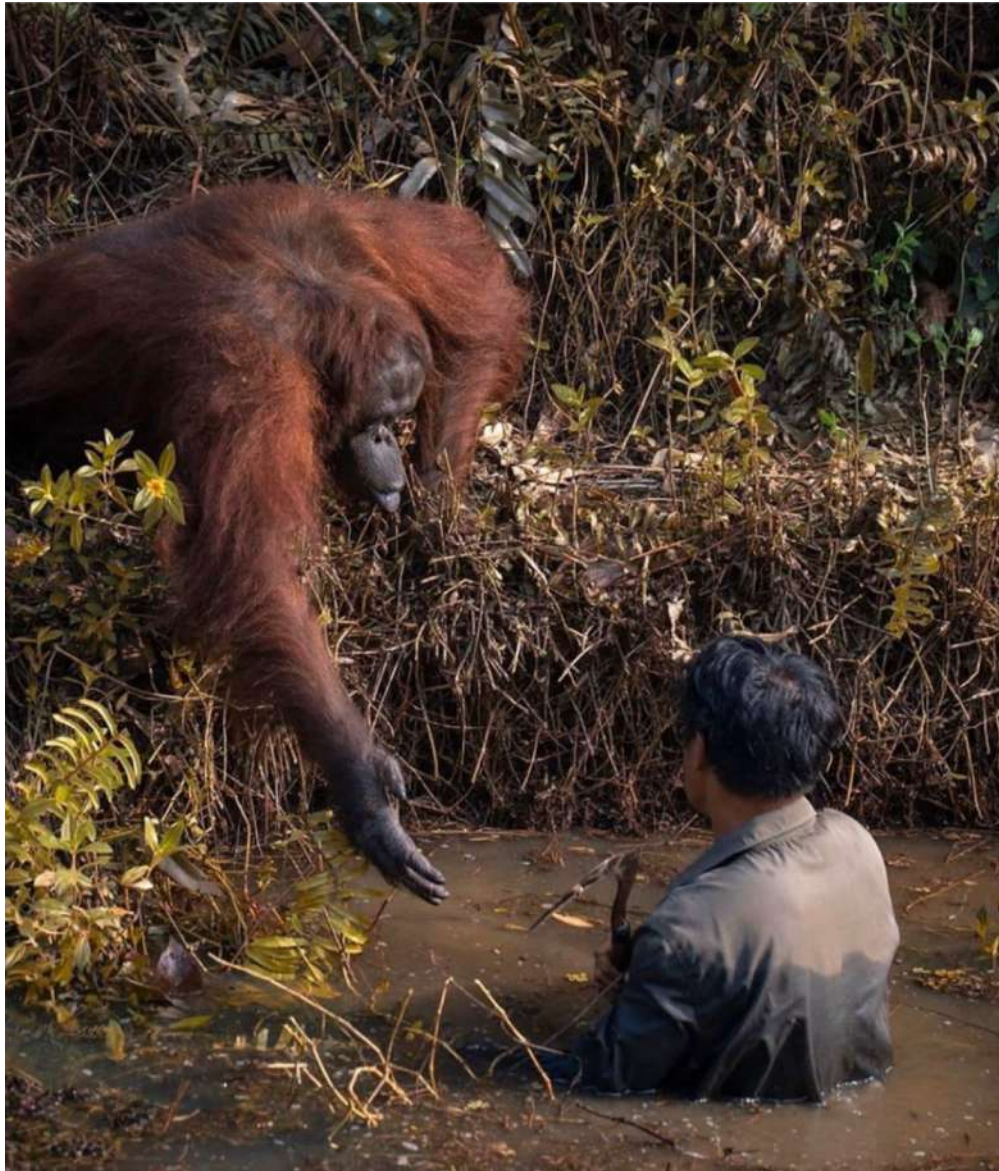
Al Rispettosa dell'Ambiente



Al Rispettosa della verità e della realtà



Primo passo è



Allineamento

Allineamento di obiettivi tra tutte le varie intelligenze artificiali e l'Uomo per salvarsi entrambi dai rischi della giungla digitale

Stiamo vivendo un'epoca di straordinaria trasformazione ...

Opportunità



perchè sia ricordata come l'alba di un nuovo Giorno,
gestiamone correttamente i rischi

the art of creating innovative solutions



Thank You

