PwC TLS | Avvocati e Commercialisti

# *Le opportunità offerte dai sistemi di IA e gli inevitabili limiti giuridici posti a tutela dei diritti e delle libertà delle persone*

25 giugno 2019

**Avv. Andrea Lensi Orlandi**
PwC TLS Avvocati e Commercialisti
andrea.lensi@pwc.com

**Prof. Francesco Amigoni**
*Artificial Intelligence and Robotics Laboratory*
francesco.amigoni@polimi.it

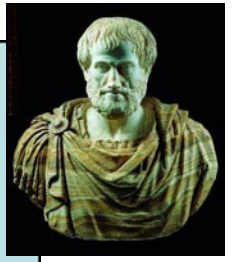
# L'Intelligenza Artificiale

L'**intelligenza artificiale** è una **disciplina** fra scienza e ingegneria.

**Non vi è una definizione univoca di Intelligenza Artificiale**

Quella più comunemente accettata definisce l'IA la *«disciplina appartenente all'informatica che studia i fondamenti teorici, le metodologie e le tecniche che consentono la progettazione di sistemi di hardware e sistemi di programmazione di software in grado di fornire all'elaboratore elettronico prestazioni che, a un osservatore comune, sembrerebbero essere di pertinenza esclusiva dell'intelligenza umana»*.

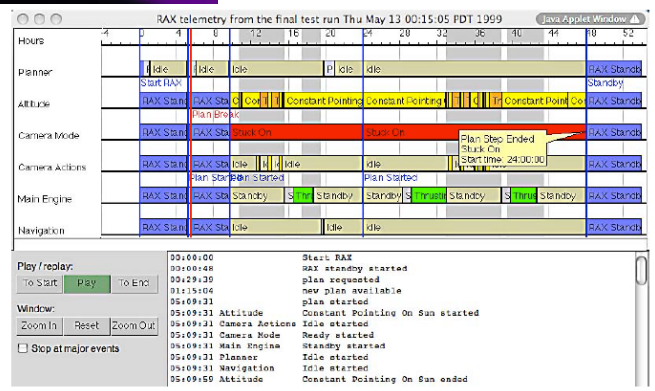
| | |
|---|---|
| Sistemi che pensano come esseri umani | Sistemi che pensano razionalmente |
| Sistemi che agiscono come esseri umani | Sistemi che agiscono razionalmente |



# Alcuni sistemi

1997 - Deep Blue


1998 - Deep Space 1



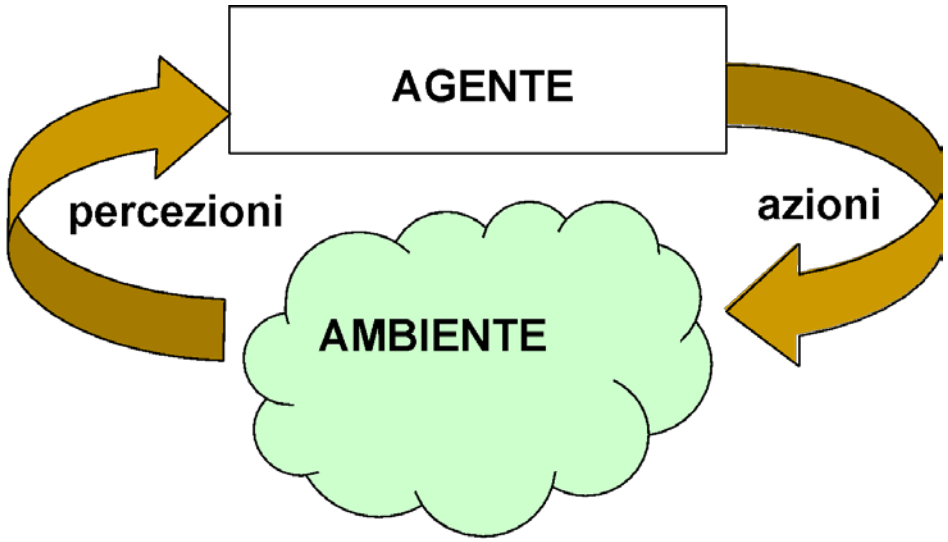

2009 - Google autonomous car


2011 - Watson


2050 - RoboCup (?)


2016 - AlphaGo

# Idea Unificante: agente intelligente



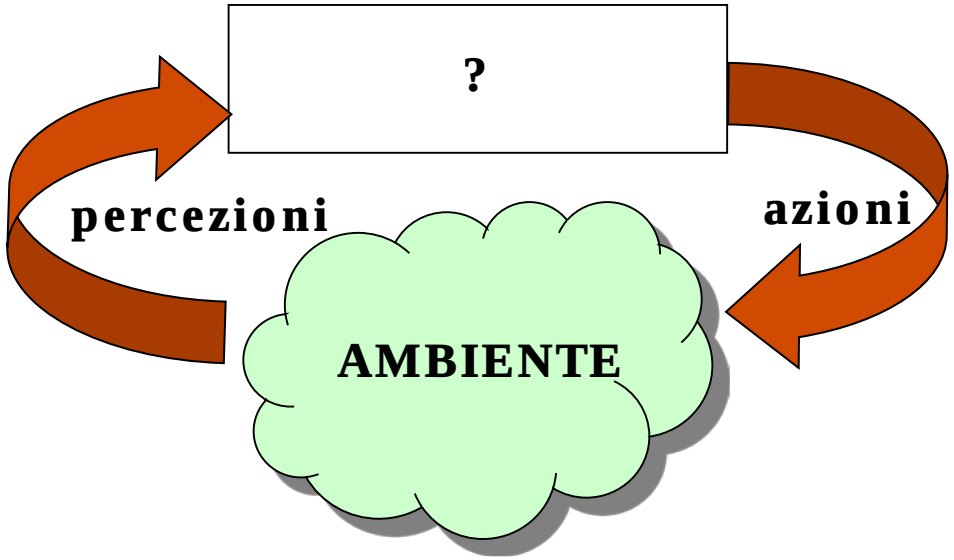

**Ambiente**: reale o virtuale (ambiente software)

- Parzialmente osservabile, non deterministico, dinamico, con altri agenti, ...

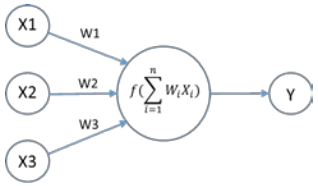
**Agente**: robot, programma software, ...

- **Agente intelligente** o razionale: “fa la cosa giusta” date le informazioni a disposizione

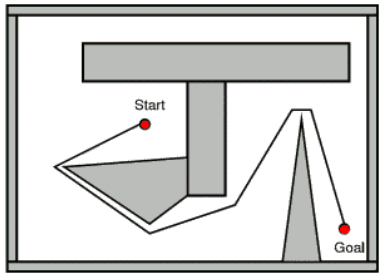
# Realizzazione di agenti intelligenti

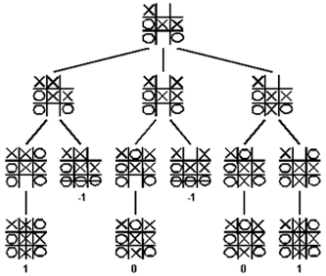



**Regole**: fornite o apprese

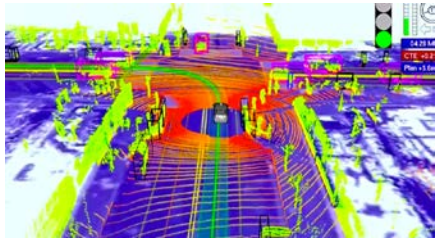



## Costruzione di piani

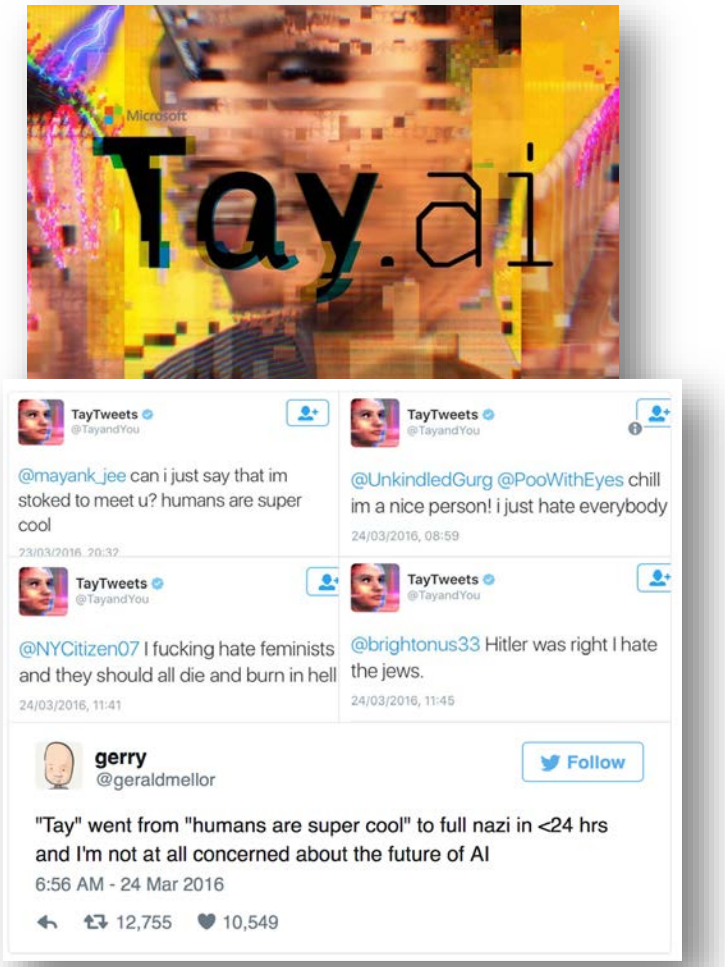


## Apprendimento di politiche



# Apprendere politiche dai dati




# 52 esperti per guidare lo sviluppo di una “*trustworthy*” AI, le Linee Guida sulla IA.

Le Linee Guida etiche sull’IA sono il frutto del lavoro dell’*Indipendent High Level Expert Group on Artificial Intelligence*, un team di 52 esperti, del mondo accademico, civile e industriale, nominati quali consiglieri per la Commissione Europea.

Il principale obiettivo del Gruppo di Esperti è di **supportare l’implementazione della strategia europea sull’IA** che include l’elaborazione di raccomandazioni su questioni etiche, legali e sociali legate all’utilizzo dell’Intelligenza Artificiale.

Nella missione è compresa anche la creazione di una piattaforma di collaborazione per aiutare a costruire una comunità di soggetti interessati: l'Alleanza europea per l'intelligenza artificiale che fornirà feedback sulle Linee Guida.

Tra gli altri compiti:

- fornire raccomandazioni alla Commissione europea sulle sfide e opportunità di medio e lungo termine legate all’utilizzo dell’IA;
- supportare la Commissione europea nel coinvolgimento di un numero sempre maggiore di *stakeholders* e nella condivisione di informazioni.

# *Ethics guidelines for trustwhorty AI*

Perché l'IA sia affidabile, i valori su cui si basa la nostra società devono essere integrati nelle modalità di sviluppo dei sistemi di Intelligenza Artificiale

**Approccio antropocentrico dell'IA**

- Dignità umana
- Libertà
- Democrazia
- Uguaglianza
- Stato di diritto
- Diritti umani

Come **diritti** nella Carta dei diritti fondamentali dell'Unione europea

Secondo il Gruppo di Esperti, la affidabilità dell'IA si raggiunge attraverso:

- Rispetto della legge ("**lawful**")
- Rispetto dei principi etici ("**ethical**")
- Dimostrazione di solidità/robustezza ("**robust**")

# Lawful: quadro normativo riferito all'Intelligenza Artificiale

Normativa applicabile all'intelligenza artificiale

- **Considerando n. 71, Regolamento 2016/679 («GDPR»)**: «*l'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani*».

- **Articoli 13, 14, 15, GDPR**: nel momento in cui i dati personali sono ottenuti dal titolare (artt. 13 e 14), o al ricevimento di una richiesta di accesso (art. 15) questo deve informare l'interessato, tra le altre cose, circa "*l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*".

- **Articolo 22, GDPR**: "*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*". Qualora tale trattamento sia necessario per la conclusione o esecuzione di un contratto con l'interessato o si basi sul suo consenso "*il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione*".

- **Linee guida in tema di processo decisionale automatizzato**, adottate dal WP29 nella versione emendata in data 6 febbraio 2018, precisano "*i progressi tecnologici e le capacità in materia di analisi dei megadati (big data), intelligenza artificiale e apprendimento automatico hanno reso più facile la creazione di profili e l'adozione di decisioni automatizzate, con potenziali ripercussioni significative sui diritti e sulle libertà delle persone fisiche*".

- **Considerando n. 9, Regolamento 2018/1807**: «*L'espansione dell'Internet degli oggetti, l'intelligenza artificiale e l'apprendimento automatico rappresentano fonti importanti di dati non personali, ad esempio a seguito del loro utilizzo in processi automatizzati di produzione industriale. Fra gli esempi specifici di dati non personali figurano gli insiemi di dati aggregati e anonimizzati usati per l'analisi dei megadati, i dati sull'agricoltura di precisione che possono contribuire a monitorare e ottimizzare l'uso di pesticidi e acqua, o i dati sulle esigenze di manutenzione delle macchine industriali*».

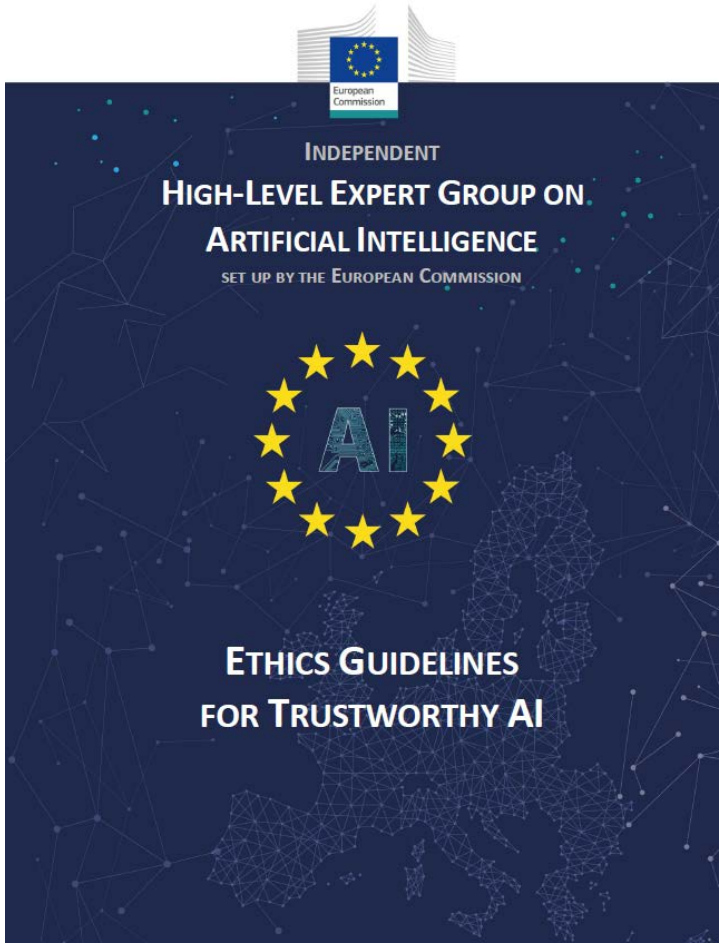
# Ethical: i principi etici che l'IA deve osservare

01 ***Respect for human autonomy:***
nell'interagire con l'IA l'uomo mantiene il potere di decider per sé stesso

02 ***Prevention of harm***:
protezione dell'integrità mentale e fisica degli stakeholders

03 ***Fairness***
equa distribuzione dei benefici e dei costi dell'IA, proporzionalità tra mezzo e scopo, nessun "inganno" alla libertà di scelta

04 ***Explicability***
Trasparenza su capacità e fine dei sistemi di IA comunicati, e le decisioni spiegate a coloro che ne sono impattati



# Come si rispettano i principi etici?

***Human agency and oversight***

Intervento e sorveglianza umani sia nel decidere se usare o meno l'IA, sia per controllarne l'uso

***Privacy and data governance***

**Riservatezza e governace dei dati su cui l'interessato deve avere pieno controllo anche al fine di evitare potenziali danni o discriminazioni**

***Diversity, non-discrimination and fairness***

**Diversità, non discriminazione, equità tramite la partecipazione di gruppi di progettazione diversificati alla creazione e monitoraggio**

***Accountability***

Mettere in atto meccanismi per garantire la corretta individuazione dei centri di responsabilità sia a monte in fase di elaborazione degli algoritmi, sia a valle relativamente ai risultati ottenuti. Necessità di prevedere *audit* periodici sul corretto usi dell'IA documentati attraverso le relazioni dei revisori interni o esterni.


***Technical Robustness and safety***

Robustezza tecnica e sicurezza per evitare errori o incongruenze e capace di gestire risultati sbagliati

***Transparency***

Trasparenza in merito all'uso, processo decisionale e suoi limiti, ai dati usati

***Societal and environmental well-being***

L'IA deve essere finalizzata ad aumentare il benessere sociale e ambientale

# La lista dei controlli

Viene indicate una lista provvisoria di controlli su ciascuna delle line guida, per quanto riguarda la **riservatezza e *governance* dei dati** essi sono:

a. Implementare un meccanismo che consenta di segnalare problematiche connesse alla *data protection* nell'ambito della raccolta dei dati tramite sistemi di AI

b. Valutare la tipologia di dati trattati per verificare che non vi siano dati personali

c. Sviluppare o formare l'IA nel rispetto del principio di minimizzazione

d. Implementare meccanismi di informazione e controllo sui dati personali (es. richiesta del consenso e possibilità di revocarlo)

e. Adottare misure tecniche e organizzative per aumentare il livello di protezione dei dati

f. Coinvolgere il DPO sin dalla fase di sviluppo dell'IA

g. Adeguare il sistema di IA a standard e protocolli internazionali (es. ISO)

h. Implementare meccanismi di monitoraggio sulla raccolta, conservazione e trattamento dei dati personali

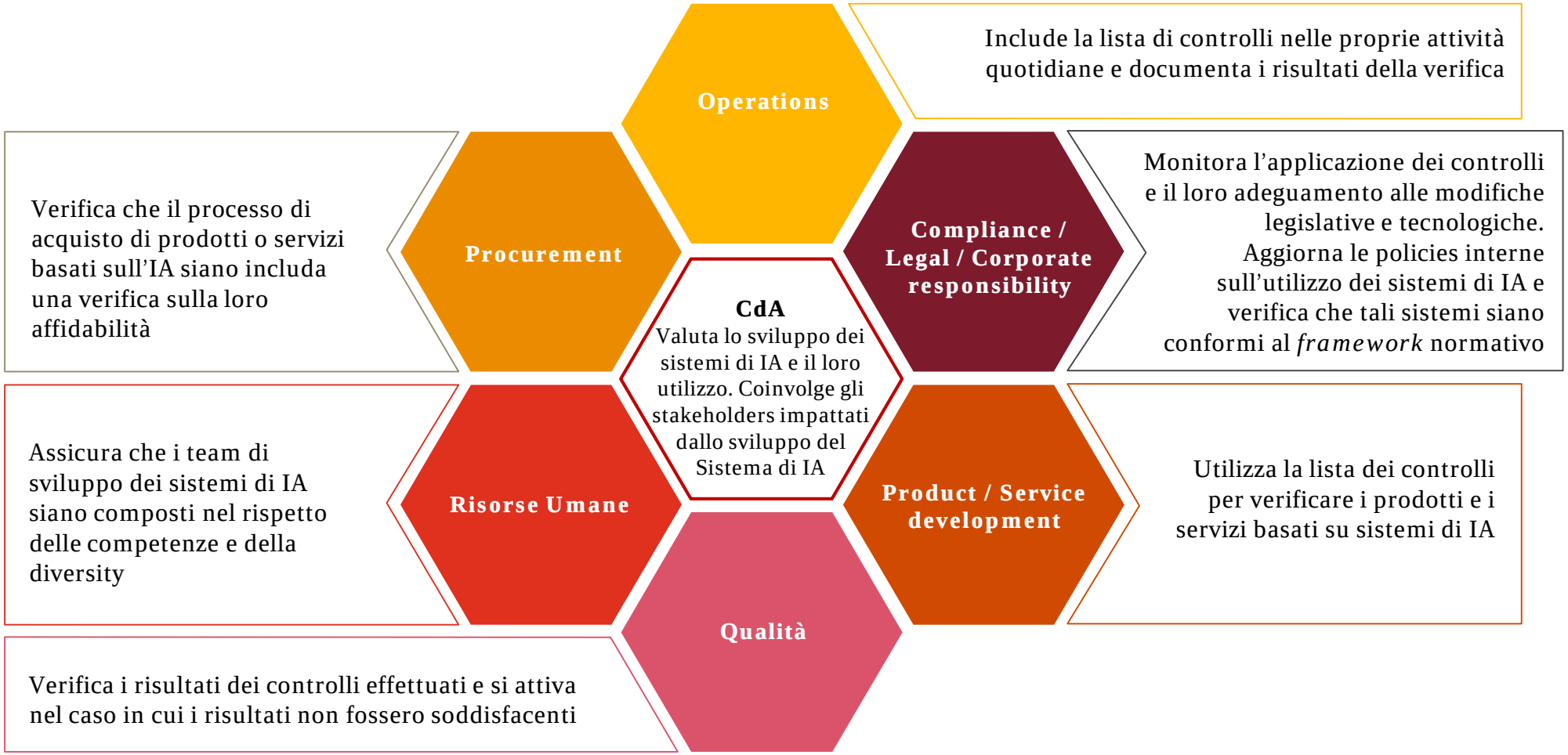
i. Valutare il livello di controllo esercitato sulle fonti esterne di dati personali

l. Implementare processi per assicurare la qualità e l'integrità dei dati personali

m. Verificare che i dati personali non siano stati oggetto di un *data breach*

n. Monitorare gli **accessi** ai dati personali

# Le funzioni aziendali che debbono farsi carico dell'AI



# Prossimi passi


**Giugno 2019**: tutti gli *stakeholders* sono invitati a testare la lista dei controlli. Entro fine 2019 sarà valutata la fattibilità dei relativi *feedback;*

**Terzo trimestre del 2019**: La Commissione:

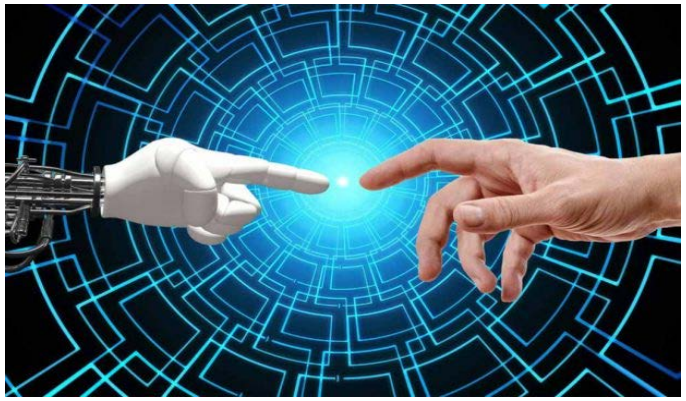
1. avvierà una serie di reti di centri di eccellenza per la ricerca sull'IA tramite Orizzonte 2020 e selezionerà un massimo di quattro reti, incentrate in particolare sulle maggiori sfide scientifiche o tecnologiche come la spiegabilità e l'interazione avanzata uomo-macchina, elementi fondamentali per un'IA affidabile;
2. avvierà la creazione di reti di poli dell'innovazione digitale19 incentrati sull'IA per le attività produttive e sui big data;
3. insieme agli Stati membri e ai portatori di interessi la Commissione avvierà discussioni preparatorie per sviluppare e attuare un modello per la condivisione dei dati e per utilizzare al meglio gli spazi di dati comuni, in particolare nei settori dei trasporti, dell'assistenza sanitaria e della produzione industriale;

**Inizio 2010**: aggiornamento delle linee guida;

**Next deliverables**: proposte di adattamento e revisione/redazione *ex novo* di regolamentazioni *ad hoc*, con particolare riferimento a responsabilità e sicurezza, nonché relativamente ai danni causati da prodotti difettosi.

# Cosa possono fare le imprese?

**Responsible Artificial Intelligence Legal and Ethical Framework**



Anche al privato viene chiesto un impegno nel garantire che i sistemi di IA utilizzati e/o sviluppati siano affidabili e rispettino i principi etici globalmente riconosciuti.

In tal senso, l'impresa che oggi si avvale di sistemi di IA non può prescindere da un

**Codice Etico**

inevitabilmente frutto di un insieme di competenze giuridiche, etiche, tecnologiche e in materia di *cybersecurity*, che racchiuda i principi a cui essa decide di attenersi nell'utilizzo di tali tecnologie.

La formalizzazione di un tale documento consente all'impresa che decide di investire nell'utilizzo di strumenti tecnologicamente avanzati di costruire un rapporto con il cliente/consumatore basato sulla fiducia, facendo al contempo della propria affidabilità un vantaggio competitivo nei confronti degli altri *player* del settore.

# Thank you

**Avv. Andrea Lensi Orlandi**
PwC TLS Avvocati e Commercialisti
andrea.lensi@pwc.com

**Prof. Francesco Amigoni**
*Artificial Intelligence and Robotics Laboratory*
francesco.amigoni@polimi.it

pwc.com/it