Intelligenza Artificiale

TRACCIA PER I CORSISTI DELLA SSPL
DELL'UNIVERSITÀ MEDITERRANEA DI REGGIO CALABRIA
I ANNO – A.A. 2021/2022

Intelligenza Artificiale

L’intelligenza artificiale studia i fondamenti teorici, le metodologie e le tecniche che consentono di progettare sistemi hardware e sistemi di programmi software atti a fornire all’elaboratore elettronico prestazioni che, a un osservatore comune, sembrerebbero essere di pertinenza esclusiva dell’intelligenza umana

(http://www.treccani.it)

Sistema intelligente → Sviluppo teoremi matematici sempre più complessi

Sistema esperto → Elaborazione di specifiche soluzioni dai dati

Algoritmo di apprendimento per reti neurali

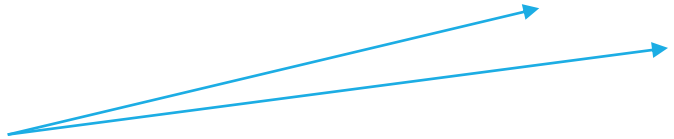
Definizione di rete neurale artificiale

Una rete neurale (in inglese *neural network*) è un modello matematico composto da neuroni artificiali di ispirazione alle reti neurali biologiche (quella umana o animale) e viene utilizzate per risolvere problemi ingegneristici di Intelligenza Artificiale legati a diversi ambiti tecnologici come l'informatica, l'elettronica o altre discipline.

(www.ionos.it)

11 maggio 1997 : scacco matto all'intelligenza umana?

Conoscenza



Conoscenza di base

Conoscenza esperienziale

Coscienza

Problem solving

Trasferimento della conoscenza alla macchina:

a) Teoria dei linguaggi formali

b) Teoria delle decisioni

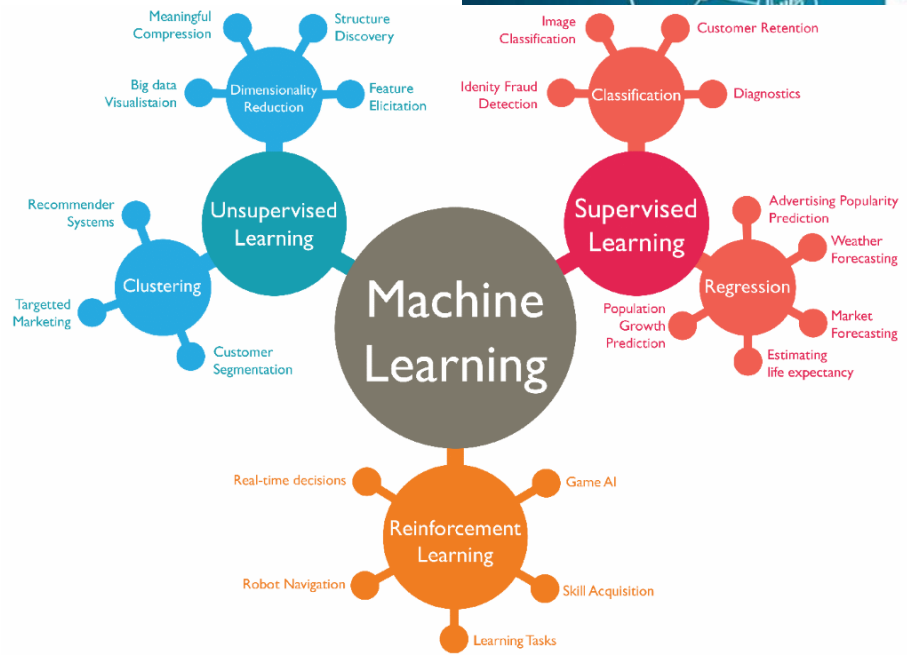
(modelli predittivi da informazioni iniziali di partenza: importanza dei dati!)

Machine learning – apprendimento automatico

Apprendimento supervisionato

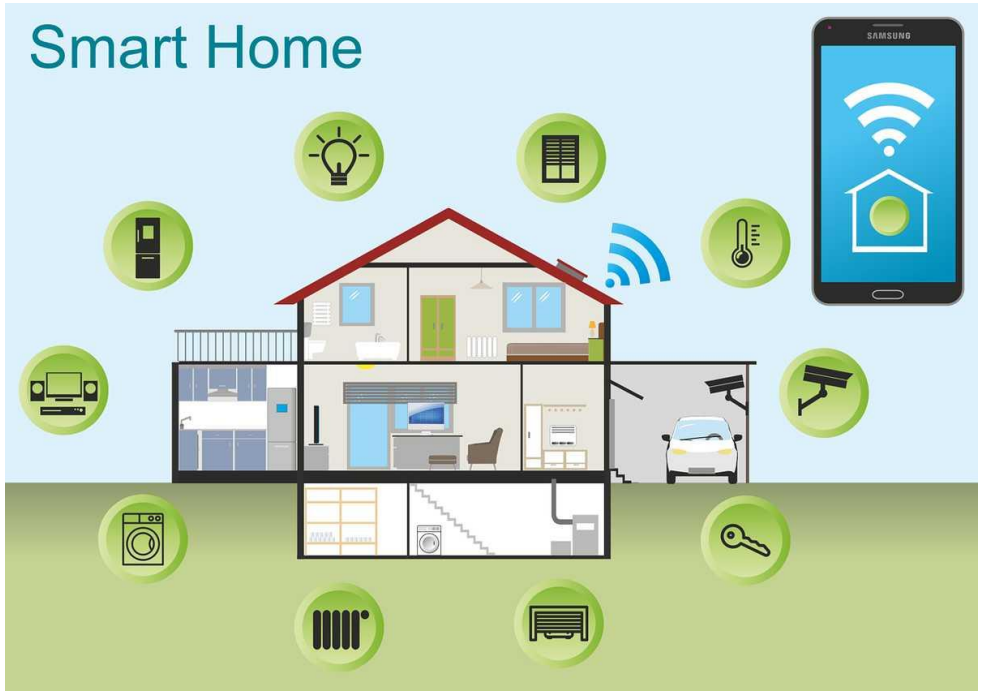
Apprendimento non supervisionato

Apprendimento «per rinforzo»



Applicazioni e Sistemi AI nel quotidiano

Domotica & smart vehicles



Trans-umanesimo : AI e diritti della persona

Superamento delle barriere dell'umano?

Potenziamento del corpo

Potenziamento della mente

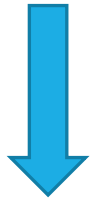
Limite dell'art. 5 cc.?

Human enhancement

Autodeterminazione : disporre di sé e del proprio corpo

Diritto a potenziarsi?

Emersione di nuove forme di diseguaglianza?



Limite invalicabile della condizione umana

AI e circolazione dei dati

I sistemi Ai si nutrono di dati

a) complessi

b) affidabili

c) provenienti da fonti diverse

Problema della

«Qualità del dato»

I sistemi AI pongono in essere una molteplicità di **trattamenti automatizzati**

Se si tratta di dati personali l'art.22 GDPR è sufficiente?

La «sfida tecnologica» dell'AI

Potere tecnologico come potere complesso

↓

Sviluppo sistemi AI e ricadute su diversi e specifici settori

della vita delle comunità

↓

Necessità di una *governance* «auspicabilmente globale» che determini implicazioni e conseguenze giuridiche ed etiche

↓

Ricerca delle regole condivise

EUR-Lex
Access to European Union law

Proposta di

Dichiarazione di cooperazione su AI (aprile 2018)

Linee Guida Etiche finali per una AI affidabile (aprile 2019)

Rapporto sulla responsabilità per AI ed altre tecnologie emergenti (novembre 2019)

Consultazione pubblica sul Libro Bianco sull'AI (febbraio 2020)

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO CHE STABILISCE REGOLE ARMONIZZATE SULL'INTELLIGENZA ARTIFICIALE (LEGGE SULL'INTELLIGENZA ARTIFICIALE) E MODIFICA ALCUNI ATTI LEGISLATIVI DELL'UNIONE

1) Armonizzare la normativa applicabile

2) Migliorare il funzionamento del mercato interno

3) Promuovere:

Innovazione

Sicurezza

Tutela dei diritti individuali

Considerando n.1

Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, la commercializzazione e l'uso dell'intelligenza artificiale (IA) in conformità ai valori dell'Unione. Il presente regolamento persegue una serie di motivi imperativi di interesse pubblico, quali un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali, e garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del presente regolamento.

Proposta di Regolamento – ART. 1

Il presente regolamento stabilisce:

regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di intelligenza artificiale ("sistemi di IA") nell'Unione;

il divieto di determinate pratiche di intelligenza artificiale;

requisiti specifici per i sistemi di IA ad alto rischio e obblighi per gli operatori di tali sistemi;

regole di trasparenza armonizzate per i sistemi di IA destinati a interagire con le persone fisiche, i sistemi di riconoscimento delle emozioni, i sistemi di categorizzazione biometrica e i sistemi di IA utilizzati per generare o manipolare immagini o contenuti audio o video;

regole in materia di monitoraggio e vigilanza del mercato.

Il Regolamento si applicherà a

immissione sul mercato

messa a disposizione sul mercato

messa in servizio

uso

dei

sistemi di Intelligenza Artificiale (*)

Prima messa a disposizione sul mercato

Qualsiasi fornitura di sistema AI per la distribuzione o l'uso sul mercato

Fornitura diretta all'utente

In modo conforme

Sistemi di Intelligenza Artificiale

un software sviluppato con una o più delle tecniche e degli approcci elen-cati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono

(art. 3 comma I, lett.a)

AI: RISK CLASSIFICATION

Rischio Massimo : divieto di immissione sul mercato, messa in servizio ed uso (art.5)

Rischio Alto: possono avere ripercussioni negative; possono essere immesse sul mercato e distribuite in determinati casi e solo a seguito di una valutazione di conformità e del rispetto di stringenti obblighi (art.6 ss.; intero Titolo III)

Rischio Limitato: minimi e precisi obblighi di trasparenza; gli utenti devono essere consapevoli che stanno interagendo con una macchina (art.52)

Rischio Minimo: sviluppati, immessi sul mercato ed utilizzati nel rispetto della legislazione vigente

Sistemi AI ad alto rischio

Regole di classificazione

Requisiti *(obbligo di conformità)*

Sistema di gestione dei rischi

Dati e governance dei dati

Trasparenza e fornitura di informazioni agli utenti

Sorveglianza umana

Obblighi dei fornitori e degli utenti

Accountability

I fornitori devono:

Dimostrare conformità del sistema ad alto rischio

Notificare ogni malfunzionamento o «serio incidente» che possa determinare violazione degli obblighi previsti dall'UE

Articolo 10
Dati e governance dei dati

1. I sistemi di IA ad alto rischio che utilizzano tecniche che prevedono l'uso di dati per l'addestramento di modelli sono sviluppati sulla base di set di dati di addestramento, convalida e prova che soddisfano i criteri di qualità di cui ai paragrafi da 2 a 5.

2. I set di dati di addestramento, convalida e prova sono soggetti ad adeguate pratiche di governance e gestione dei dati. Tali pratiche riguardano in particolare:

   a) le scelte progettuali pertinenti;

   b) la raccolta dei dati;

   c) le operazioni di trattamento pertinenti ai fini della preparazione dei dati, quali annotazione, etichettatura, pulizia, arricchimento e aggregazione;

   d) la formulazione di ipotesi pertinenti, in particolare per quanto riguarda le informazioni che si presume che i dati misurino e rappresentino;

   e) una valutazione preliminare della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari;

   f) un esame atto a valutare le possibili distorsioni;

   g) l'individuazione di eventuali lacune o carenze nei dati e il modo in cui tali lacune e carenze possono essere colmate.

3. I set di dati di addestramento, convalida e prova devono essere pertinenti, rappresentativi, esenti da errori e completi. Essi possiedono le proprietà statistiche appropriate, anche, ove applicabile, per quanto riguarda le persone o i gruppi di persone sui quali il sistema di IA ad alto rischio è destinato a essere usato. Queste caratteristiche dei set di dati possono essere soddisfatte a livello di singoli set di dati o di una combinazione degli stessi.

4. I set di dati di addestramento, convalida e prova tengono conto, nella misura necessaria per la finalità prevista, delle caratteristiche o degli elementi particolari dello specifico contesto geografico, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere usato.

5. Nella misura in cui ciò sia strettamente necessario al fine di garantire il monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio, i fornitori di tali sistemi possono trattare categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, all'articolo 10 della direttiva (UE) 2016/680 e all'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725, fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche, comprese le limitazioni tecniche all'utilizzo e al riutilizzo delle misure più avanzate di sicurezza e di tutela della vita privata, quali la pseudonimizzazione o la cifratura, qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita.

6. Per lo sviluppo di sistemi di IA ad alto rischio diversi da quelli che utilizzano tecniche che prevedono l'addestramento di modelli si applicano adeguate pratiche di gestione e governance dei dati, al fine di garantire che tali sistemi di IA ad alto rischio siano conformi al paragrafo 2.

Articolo 13
Trasparenza e fornitura di informazioni agli utenti

1. I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare l'output del sistema e utilizzarlo adeguatamente. Sono garantiti un tipo e un livello di trasparenza adeguati, che consentano di conseguire il rispetto dei pertinenti obblighi dell'utente e del fornitore di cui al capo 3 del presente titolo.

2. I sistemi di IA ad alto rischio sono accompagnati da istruzioni per l'uso in un formato digitale o non digitale appropriato, che comprendono informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili per gli utenti.

3. Le informazioni di cui al paragrafo 2 specificano:

   a) l'identità e i dati di contatto del fornitore e, ove applicabile, del suo rappresentante autorizzato;

   b) le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio, tra cui:

      i) la finalità prevista;

      ii) il livello di accuratezza, robustezza e cibersicurezza di cui all'articolo 15 rispetto al quale il sistema di IA ad alto rischio è stato sottoposto a prova e convalidato e che ci si può attendere, e qualsiasi circostanza nota e prevedibile che possa avere un impatto sul livello atteso di accuratezza, robustezza e cibersicurezza;

      iii) qualsiasi circostanza nota o prevedibile connessa all'uso del sistema di IA ad alto rischio in conformità alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, che possa comportare rischi per la salute e la sicurezza o per i diritti fondamentali;

      iv) le sue prestazioni per quanto riguarda le persone o i gruppi di persone sui quali il sistema è destinato a essere utilizzato;

      v) ove opportuno, le specifiche per i dati di input o qualsiasi altra informazione pertinente in termini di set di dati di addestramento, convalida e prova, tenendo conto della finalità prevista del sistema di IA;

   c) le eventuali modifiche apportate al sistema di IA ad alto rischio e alle sue prestazioni, che sono state predeterminate dal fornitore al momento della valutazione iniziale della conformità;

   d) le misure di sorveglianza umana di cui all'articolo 14, comprese le misure tecniche poste in essere per facilitare l'interpretazione degli output dei sistemi di IA da parte degli utenti;

   e) la durata prevista del sistema di IA ad alto rischio e tutte le misure di manutenzione e cura necessarie per garantire il corretto funzionamento di tale sistema, anche per quanto riguarda gli aggiornamenti software.

Garantire
il principio di trasparenza e l'informazione

Ma quali informazione è realmente possibile fornire all'utente?

Quale grado in intellegibilità deve/può essere garantito?

Quale grado in intellegibilità deve/può essere compreso?

Ue Regulation – Artificial Intelligence ACT

Regolamento UE può essere lo strumento migliore?

Regolamento UE potrà risolvere/regolare tutte le criticità attuali in tema di AI?

Regolamento UE potrà superare le criticità dell'art.22 GDPR?

Indicazioni bibliografiche:

Alpa, «Quale modello normativo per l'intelligenza artificiale?» in Contratto e Impresa, 2021, p. 1003 ss.

Alpa (a cura di), Diritto e intelligenza artificiale, Ed. Pacini, 2020

Ruffolo (a cura di), Intelligenza artificiale. Il diritto, i diritti, l'etica, Ed. Giuffrè, 2020

Signorelli, «La prevedibilità della e nella decisione giudiziaria» in AA.VV. Il diritto nell'era digitale, Ed. Giuffrè, 2022, p. 997 ss.

Quattrocolo, «Intelligenza artificiale e giustizia nella cornice della Carta Etica Europea. Gli spunti per un'urgente discussione tra scienze penali e informatiche», in La legislazione penale, 2018, fasc. 12

Casonato-Marchetti, «Prime osservazioni sulla proposta di regolamento della Commissione UE in materia di intelligenza artificiale», in Bio-Law Journal-Rivista di BioDiritto, 2021, p. 415 ss.