UNIVERSITÀ DEGLI STUDI “MAGNA GRAECIA DI CATANZARO”
Corso di INFORMATICA GIURIDICA
DOCENTE: Avv. Prof. FABRIZIO SIGILLÒ - A.A. 2026/2027

# INTRODUZIONE ALLA CONOSCENZA DELL’INTELLIGENZA ARTIFICIALE


LA STORIA E L'EVOLUZIONE DELL'INTELLIGENZA ARTIFICIALE ..... 4
1. DEFINIZIONE DELL'IA ..... 4
2. LE ORIGINI FILOSOFICHE E LETTERARIE ..... 5
MITO E FILOSOFIA ANTICA ..... 5
FILOSOFIA DI ARISTOTELE: LA LOGICA FORMALE, I SILLOGISMI E IL CONCETTO DI "RAGIONAMENTO". ..... 5
3. LA NASCITA DELL'INTELLIGENZA ARTIFICIALE MODERNA (ANNI '40) ..... 6
ALAN TURING ..... 6
IL TEST DI TURING ..... 6
4. IL PERIODO DEL DOPOGUERRA ..... 7
5. LA RINASCITA DELL'IA (ANNI '90 - PRIMI 2000) ..... 7
6. L'ERA MODERNA DELL'I.A. (DA MACHINE LEARNING A DEEP LEARNING) ..... 8
7. INTRODUZIONE ALL'INTELLIGENZA ARTIFICIALE COME OBIETTIVO PER IL PROBLEM SOLVING ..... 8
8. LA LOGICA FORMALE ..... 9
IA SIMBOLICA ..... 9
IA CONNESSIONISTA ..... 9
IA EVOLUTIVA ..... 9
9. COME FUNZIONANO I SISTEMI DI INTELLIGENZA ARTIFICIALI? ..... 9
10. TECNICHE DI APPRENDIMENTO AUTOMATICO (O MACHINE LEARNING) ..... 10
ALGORITMO ..... 10
MODELLO ..... 10
APPRENDIMENTO SUPERVISIONATO (SUPERVISED LEARNING) ..... 11
APPRENDIMENTO NON SUPERVISIONATO (UNSUPERVISED LEARNING) ..... 11
APPRENDIMENTO PER RINFORZO (REINFORCEMENT LEARNING) ..... 12
FASI DEL PROCESSO DI APPRENDIMENTO AUTOMATICO ..... 12
11. APPLICAZIONI DELL'INTELLIGENZA ARTIFICIALE ..... 12
L'INTELLIGENZA ARTIFICIALE NEL SETTORE GIURIDICO ..... 13
GLI ERRORI DEL SISTEMA DI INTELLIGENZA ARTIFICIALE ..... 13
ALLUCINAZIONI ..... 13
BIAS ..... 14

INTRODUZIONE ALLA CONOSCENZA DELL’INTELLIGENZA ARTIFICIALE

RIDURRE ED ELIMINARE IL BIAS? ..... 15
LA GESTIONE E LA TUTELA DEI DATI PERSONALI ..... 15
L'INTELLIGENZA ARTIFICIALE NEL SETTORE SANITARIO ..... 16
L'INTELLIGENZA ARTIFICIALE NEL SETTORE LAVORATIVO ..... 16
12. ALTRI SETTORI ..... 17
AMBITO FINANZIARIO ..... 17
MARKETING E COMMERCIO ..... 17
MOBILITÀ ..... 17
I RAPPORTI UMANI ..... 17
13. LE ESPERIENZE GIURIDICHE SULL'INTELLIGENZA ARTIFICIALE NEI VARI PAESI ..... 18
STATI UNITI ..... 18
CINA ..... 18
CANADA ..... 18
REGNO UNITO ..... 18
UNIONE EUROPEA ..... 18
REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE (AI ACT): PRINCIPI E STRUTTURA ..... 19
FRIA (Fundamental Rights Impact Assessment). ..... 19
LE SANZIONI EUROPEE. ..... 19
OBBLIGHI DI PROVIDER E DEPLOYER. ..... 19
REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (GDPR) ..... 20
DIRETTIVA SULLA RESPONSABILITÀ PER DANNI CAUSATI DA IA (AI LIABILITY DIRECTIVE) ..... 20
14. L'APPROCCIO GIURIDICO DELLO STATO ITALIANO ALL'IA ..... 20
15. LEGGE 132/2025 ..... 21
FINALITÀ PRINCIPALI (ART. 1) ..... 21
RAPPORTO CON IL REGOLAMENTO UE (ART. 1, COMMA 2) ..... 22
PARTE II - PRINCIPI GENERALI E DEFINIZIONI ..... 22
DEFINIZIONI FONDAMENTALI (ART. 2) ..... 22
PRIVACY E PROTEZIONE DATI (ART. 4) ..... 23
PARTE III - DISPOSIZIONI SETTORIALI ..... 23

SANITÀ E DISABILITÀ (ARTT. 7-10) ..... 23
RICERCA SCIENTIFICA (ART. 8) ..... 24
FASCICOLO SANITARIO ELETTRONICO E PIATTAFORMA IA (ART. 10) ..... 24
LAVORO ..... 24
PRINCIPI GENERALI (ART. 11) ..... 24
OSSERVATORIO NAZIONALE (ART. 12) ..... 24
PROFESSIONI INTELLETTUALI (ART. 13) ..... 25
PUBBLICA AMMINISTRAZIONE (ART. 14) ..... 25
GIUSTIZIA (ART. 15) ..... 25
SICUREZZA E DIFESA (ART. 6) ..... 26
PARTE IV - GOVERNANCE E STRATEGIA NAZIONALE ..... 26
STRATEGIA NAZIONALE PER L'IA (ART. 19) ..... 26
TUTELE E DIRITTO D'AUTORE ..... 27
TEXT AND DATA MINING (ART. 70-SEPTIES) ..... 27
DISPOSIZIONI IN MATERIA PENALE. ..... 28
AGRAVANTE GENERALE (ART. 26, LETT. A) ..... 28
DIFFUSIONE ILLECITA DI CONTENUTI IA (ART. 26, LETT. C) ..... 28
D.LGS. 179/2026 ..... 28
GLOSSARIO GIURIDICO MINIMO DELL'IA ..... 29

UNIVERSITÀ DEGLI STUDI “MAGNA GRAECIA DI CATANZARO”
Corso di INFORMATICA GIURIDICA
DOCENTE: Avv. Prof. FABRIZIO SIGILLÒ - A.A. 2026/2027

INTRODUZIONE ALLA CONOSCENZA DELL’INTELLIGENZA ARTIFICIALE

# LA STORIA E L'EVOLUZIONE DELL'INTELLIGENZA ARTIFICIALE

La tentazione di introdurre la sezione delle dispense dedicata all'intelligenza artificiale è quella di chiedere a chi legge "che cosa sia l'intelligenza artificiale".

Troppo si parla di essa, troppe le prospettive e le aspettative di un sistema che si risolve pur sempre nel contributo apportato dall'uomo e dal suo cervello e la macchina, certamente più rapida nell'esecuzione di calcolo ma pur sempre subordinata all'input che l'uomo le dà.

Parte così un discorso che si arricchisce, nel corso degli anni, di passaggi ulteriori preordinati a realizzare procedure che insegnino alla macchina ad eseguire alcune attività (ancorché complesse) e giunge alla predisposizione di sistemi che oltre all'insegnamento, consentano alla macchina di andare oltre e cioè di apprendere quel che l'uomo non ha insegnato, fino ad elaborare e proporre soluzioni definitive.

## 1. DEFINIZIONE DELL'IA

Data la premessa che precede può quindi ritenersi, in linea generale, che la IA possa definirsi come "settore della scienza informatica dedicato alla creazione di sistemi in grado di svolgere compiti che richiederebbero intelligenza umana".

Al suo interno si sviluppano sotto branche:

**IA ristretta (o debole)** che è progettata per svolgere compiti specifici (si pensi ad una applicazione che aiuta in cucina ma non sa nulla di idraulica) ed il cui esempio più tipico è rappresentato dagli assistenti virtuali disponibili sugli smartphone (Siri o Alexa) che rispondono a domande ma non vanno oltre e non sono in grado di imparare alcunché.

**IA forte (o generale)** va oltre, avvicinandosi alle capacità cognitive umane, perché può imparare ma anche assumere decisioni in modo autonomo esattamente come farebbe l'uomo e con il vantaggio di estendere la sua conoscenza non solo ad un unico settore ma ad un ambito più ampio.

**Integrazione: la definizione giuridica di "sistema di intelligenza artificiale".** La definizione sopra riportata è descrittiva e di matrice informatica. Il diritto europeo, con l'**AI Act (Regolamento UE 2024/1689)**, ha introdotto una definizione giuridicamente vincolante: è un **sistema basato su macchine** progettato per operare con un certo grado di **autonomia**, che può adattarsi dopo l'immissione in servizio e che, a partire dai dati ricevuti in input, genera **output** quali previsioni, contenuti, raccomandazioni o decisioni, al fine di raggiungere obiettivi espliciti o impliciti. La differenza rispetto alla dispensa non è terminologica: questa definizione è il presupposto per applicare gli obblighi, le classificazioni di rischio e le sanzioni di cui parleremo. La Legge 132/2025 richiama espressamente questa definizione e vi si conforma.

# 2. LE ORIGINI FILOSOFICHE E LETTERARIE

Anche in questo caso (così come è stato detto a proposito del Regolamento sul trattamento dei dati personali) erra chi ritiene che l'intelligenza artificiale debba intendersi come un processo legato all'introduzione dei computer o, comunque, dei sistemi elettronici, dacché – e pur sempre con le dovute proporzioni – l'IA trova i suoi precedenti nella più antica storia dell'uomo.

## MITO E FILOSOFIA ANTICA

Qualcosa di idealmente simile all'IA si rinviene infatti nella mitologia greca che conosceva gli "*automì*" come Talos, gigantesco automa di bronzo, invulnerabile perché il suo corpo era alimentato dal sangue degli dei, ma sintomaticamente – così come accade per gli apparecchi elettronici – vittima di un punto debole collocato in una zona della caviglia in cui si trova l'unica vena scoperta attraverso cui scorre il suo sangue.

Ed è nella filosofia greca che si rinvengono principi assolutamente compatibili che quelli posti a fondamento dell'idea di realizzare forme di intelligenza non umana.

## FILOSOFIA DI ARISTOTELE: LA LOGICA FORMALE, I SILLOGISMI E IL CONCETTO DI "RAGIONAMENTO".

Il riferimento alla filosofia aristotelica muove dal sistema di ragionamento deduttivo da quegli elaborato e che è basato sui sillogismi e cioè un argomento costituito da tre proposizioni: due premesse e una conclusione.

Premesse = si intendono affermazioni che si suppongono vere

Conclusioni = affermazioni logicamente derivanti dalle premesse.

Tipico di questi principi è il noto sillogismo su Socrate:

- Premessa 1: Tutti gli uomini sono mortali (affermazione vera)
- Premessa 2: Socrate è un uomo (2.a premessa altrettanto vera).
- Conclusione: Quindi, Socrate è mortale (conclusione irrevocabile).

Queste le basi su cui si elabora la c.d. **logica formale** che si basa sulla convinzione che il ragionamento valido può essere analizzato e formalizzato attraverso regole.

Anche in questo caso e con le dovute proporzioni si può dire che non siamo lontanissimi dalla base dell'intelligenza artificiale che affronta, per l'appunto, la possibilità di elaborazione del ragionamento nelle sue diverse componenti:

RAGIONAMENTO DEDUTTIVO:

applicazione di regole generali a casi specifici che consentono di ottenere nuove conclusioni.

RAGIONAMENTO INDUTTIVO:

generalizzazione di osservazioni specifiche poi più ampliate in modo da estendere ragionamento e conclusioni.

RAGIONAMENTO ABDUTTIVO:

individuare una spiegazione più probabile per un insieme di osservazioni.

È ovvio che la favolistica ricostruzione storico-filosofica aiuta solo a comprendere le fondamenta su cui vengono realizzati, durante la seconda guerra mondiale, applicazioni di calcolo tecnicamente più assimilabili all'attuale intelligenza artificiale.

# 3. LA NASCITA DELL'INTELLIGENZA ARTIFICIALE MODERNA (ANNI '40)

Guida l'originario interesse verso i sistemi di calcolo, il contesto socio politico mondiale compreso tra gli anni 40 (gli anni della guerra mondiale) e che prosegue fino agli anni 50 (muove cioè dal dopoguerra).

Non casualmente l'approfondimento si rivolge alle forme di crittografia, che si rivela l'idea idonea a superare, attraverso il calcolo, quei profili di segretezza che agevolavano il rapporto tra gli stati in conflitto.

È di questo periodo l'attività svolta da quello che è ritenuto ancora oggi l'ideale ideatore dell'intelligenza artificiale

## ALAN TURING

L'apporto del matematico inglese, che operò nella fase più acuta della seconda guerra mondiale, fu rivolto alla possibilità di decrittare i codici tedeschi realizzati con la macchina **Enigma** (che i lettori di queste dispense hanno già conosciuto nella parte dedicata alla firma digitale) e di creare una procedura che potesse superare, non occasionalmente, la segretezza del messaggio realizzato con essa, poi concretamente realizzato con uno specifico apparecchio denominato "**Bombe**".

Siamo ancora alle origini dell'intelligenza artificiale e che di quella attuale ha ben poco, ma contiene i suoi prodromi e cioè la possibilità di realizzare un calcolo complesso destinato a risolvere problemi complessi e che viene sottoposto ad un test preventivo al fine di accertarne l'effettivo funzionamento.

## IL TEST DI TURING

La fase di sperimentazione del progetto di Turing costituisce il primo tentativo di prova c.d. "comportamentale", basato cioè sulla convinzione che una macchina può imitare il comportamento di un essere umano in una conversazione.

Essa prevede cioè una azione diretta posta in essere da un uomo (che viene denominato interrogatore) che interagisce con due entità: una macchina e l'essere umano ma non sa se a rispondere sia la macchina o l'uomo.

Nel momento in cui l'interrogatore non riesce a distinguere la macchina dall'essere umano (molto semplicemente quando la macchina si comporta come se fosse un uomo) ed allora la macchina ha superato il test.

Si tratta di una prova valida se rapportata all'epoca ed allo scopo a cui era destinato ma i cui limiti furono presto messi a nudo. Il calcolo semplice trascurava ad esempio di considerare alcuni elementi che (come la creatività o la capacità di risolvere problemi complessi) possono influire sul risultato finale.

Ciò non toglie che il test di Turing continui ancor oggi ad essere considerato come punto di avvio dei successivi sviluppi dell'intelligenza artificiale.

# 4. IL PERIODO DEL DOPOGUERRA

Si dovrà arrivare al dopoguerra per tracciare lo storico ed ufficiale passaggio alla fase di ricerca sull'intelligenza artificiale.

È un passaggio che si fa coincidere con la **Conferenza di Dartmouth tenutasi nel luglio del 1956** e che riunì alcuni dei più brillanti scienziati e matematici dell'epoca per discutere le possibilità di creare macchine in grado di pensare e imparare come gli esseri umani.

L'evento rimane storicamente rilevante sebbene non determinante allo sviluppo delle vere e proprie applicazioni ispirate ai ragionamenti matematici.

Il limite va rinvenuto soprattutto nelle difficoltà economiche verificatesi nel corso degli anni 70 e 80 che non casualmente vennero denominati "Winter" (inverno) perché coincidenti con freddi periodi caratterizzati da situazioni contingenti che portarono alla diminuzione di finanziamenti e ad un disinteresse pubblico verso l'IA, con conseguente rallentamento della ricerca e dello sviluppo e l'inevitabile ridimensionamento delle aspettative originarie, ispirate alla realizzazione di apparecchiature forse sovrastimate perché presentate come risolutive di molteplici problematiche ma che non realizzarono, in quel periodo, quegli obiettivi anche perché la tecnologia dell'epoca non ancora avanzata come quella attuale e non era in grado di gestire quegli irrinunciabili calcoli complessi.

# 5. LA RINASCITA DELL'IA (ANNI '90 - PRIMI 2000)

È proprio con il diffondersi di macchine sempre più performanti e suscettibili di accelerare le procedure di calcolo che si assiste, a partire dalla fine degli anni 90 e successivi, un periodo di rinascita dell'IA.

Segnali utili in tal senso pervennero da contesti per alcuni versi singolari perché estranei agli obiettivi che le macchine artificiali si promettevano di realizzare. Significativo, tra questi, l'esito della sfida scacchistica tra il campione del mondo Kasparov ed un computer realizzato da IBM e denominato "**Deep blue**" che viene annoverato quindi come primo esempio concreto della possibilità, per una macchina, di superare l'uomo in compiti complessi.

Il ruolo della statistica e del machine learning

La possibilità di insegnare ad una macchina a giocare a scacchi, convinse della possibilità di poter insegnare dati sempre più ampi addestrando la macchina all'esecuzione di procedure sempre più complesse (machine learning).

# 6. L'ERA MODERNA DELL'I.A. (DA MACHINE LEARNING A DEEP LEARNING)

È attraverso questi passaggi che si giunge ai giorni nostri, caratterizzati dall'intenzione di esasperare ancora di più la fase di addestramento e di realizzare quell'approfondimento ulteriore che sarà definito "**deep learning**".

Si tratta del perfezionamento del precedente "**machine learning**" di cui si era sopra detto e che è ispirato da un **apprendimento profondo** (la traduzione è in questo caso letterale) realizzato mediante più machine learning che utilizzano particolari reti e che, proprio in questo modo, riescono a simulare sempre meglio il potere del cervello umano, consentendo all'apparecchio di assumere una decisione sulla base di schemi sempre più ampi e di banche dati sempre più grandi.

Tra le reti di riferimento si ricorda **AlexNet** che segna un passaggio sempre più simile all'idea che oggi abbiamo dell'IA perché segna l'estensione dei sistemi alla possibilità di riconoscere immagini e video, tradurre un testo, elaborare il linguaggio naturale ed altro.

È un passaggio che si sposa con lo stesso sviluppo degli strumenti informatici che diventano sempre più accessibili e che rendono di conseguenza più disponibile anche l'IA.

Questo obiettivo trova ampio supporto nelle community open source in cui si diffusero vari strumenti (TensorFlow e PyTorch) utili all'ulteriore elaborazione di modelli di machine learning che andranno a costituire componenti già pronti per la costruzione di ulteriori sviluppi ancora più precisi.

# 7. INTRODUZIONE ALL'INTELLIGENZA ARTIFICIALE COME OBIETTIVO PER IL PROBLEM SOLVING

Premessi i profili informatici su cui si fonda l'idea di intelligenza artificiale, risulta più facile percepire le sue finalità, nettamente distinte dalla semplice realizzazione di programmi informatici che rispondono ad una domanda ed orientati – come si è detto più volte – alla

creazione di sistemi elettronici in grado di emulare alcune capacità cognitive umane al fine di migliorarle attraverso graduale aumento delle operazioni di ragionamento e con la finalità di dare risposte soddisfacenti ad un vario tipo di domande (c.d. **problem solving**).

Questo obiettivo si realizza attraverso procedure che ripropongono – debitamente adeguate ed aggiornate – quei concetti storici di "logica" che abbiamo rinvenuto nell'antica filosofia greca e che, se riferite all'IA, vengono affidate più precisamente alla "logica formale" od a "reti neurali artificiali".

# 8. LA LOGICA FORMALE

Appartengono alla logica formale modalità di sviluppo di strumenti di intelligenza artificiale denominati

## IA SIMBOLICA

Gli strumenti di IA che fanno capo alla logica simbolica si basano sull'utilizzo di simboli e regole per rappresentare il ragionamento umano che vengono applicati al fine di eseguire processi logici complessi che ripropongono il procedimento di Aristotele nelle forme del ragionamento deduttivo (da un fatto, Socrate, deduco il risultato che Socrate è un uomo e del ragionamento induttivo (pongo il fatto e comprendo cosa potrebbe accadere). Diverso è l'approccio che fa capo alla c.d.

## IA CONNESSIONISTA

Essa si fonda sull'uso delle già richiamate reti neurali artificiali tra loro connesse e che comprendono un numero variegato di modelli matematici ispirati al funzionamento del cervello umano e quindi, come il cervello umano, capaci di apprendere dati e migliorare gradualmente le loro prestazioni.

## IA EVOLUTIVA

In questo caso il riferimento sono gli algoritmi genetici e i processi di selezione naturale. In pratica il sistema crea algoritmi che apprendono automaticamente un dato e può così giungere a prevedere come si evolverà quel dato nel tempo, attingendo ad una serie di indicazioni pervenute in fase di programmazione.

# 9. COME FUNZIONANO I SISTEMI DI INTELLIGENZA ARTIFICIALI?

Se è stato detto più volte che l'IA mira ad una simulazione quanto mai fedele del ragionamento umano, attuata mediante processi intelligenti affidati a sistemi informatici, pare che il miglior modo per comprendere le modalità di funzionamento sia proprio quello che ripercorre lo sviluppo del ragionamento umano.

Esso si sviluppa nel corso degli anni di vita dell'uomo, in periodi differenti e con risultati sempre che potremmo riassumere mediante la raffigurazione di una ideale curva.

Essa parte dalla nascita e quindi la curva è bassa perché riferita a valori limitati di ragionamento; l'uomo cresce e il suo ragionamento si sviluppa gradualmente, risentendo dagli input che provengono da famiglia e scuola; procede ancora con la fase dell'adolescenza; tocca il suo culmine nell'età che definiamo della maturità e poi inizia con la fase discendente che porterà alla vecchiaia e quindi ad un ragionamento più limitato che nelle ipotesi patologiche (si pensi al Parkinson) tenderà a scomparire definitivamente.

Anche il processo con cui viene formato il cervello artificiale si realizza attraverso fasi differenti ma inevitabilmente ispirate a quelle che sono state sopra riassunte:

**apprendimento** (capacità di migliorare le prestazioni basandosi sull'esperienza);

**ragionamento**: (capacità di risolvere problemi attraverso l'analisi logica);

**auto-correzione**: (capacità di identificare e correggere errori).

Nello sviluppo del ragionamento dell'uomo si è detto che influiscono elementi esterni quale scuola o famiglia, nello sviluppo della macchina è l'uomo stesso che procede all'esecuzione delle varie fasi attraverso procedure personalizzate di istruzione.

# 10. TECNICHE DI APPRENDIMENTO AUTOMATICO (O MACHINE LEARNING)

Le definizioni che ci aiutano a comprendere il significato di machine learning ovverosia della procedura con cui la macchina viene istruita, sono algoritmo e modello

## ALGORITMO

In maniera molto sintetica l'algoritmo è un insieme di esecuzioni che viene realizzata nella fase di programmazione di una applicazione informatica e che è destinata a dire alla macchina di eseguire determinate operazioni (es. se si clicca il tasto G di Word significa che vuoi inserire il grassetto ad una parola). Il sistema esegue il compito e si ferma lì, attendendo magari altri ordini che il programmatore avrà impostato mediante ulteriore algoritmo e che verranno richiesti dall'utente (tipo vai a capo oppure salva il documento).

## MODELLO

Invece di scrivere un algoritmo il programmatore può realizzare un **modello che impara da una serie di esempi** (solo al fine di rendere più chiaro il concetto richiamando l'esempio che precede, il modello predisposto potrebbe essere che se chiedo alla macchina di salvare il file il modello prevede che apra una cartella sul desktop per inserire automaticamente dentro ad essa il file salvato).

# INTRODUZIONE ALLA CONOSCENZA DELL’INTELLIGENZA ARTIFICIALE

Parlando di uno strumento di intelligenza artificiale il tipo di apprendimento si realizza in maniera automatica e, nel caso di utilizzo di algoritmi fa capo a tre categorie principali:

## APPRENDIMENTO SUPERVISIONATO (SUPERVISED LEARNING)

La parola supervisionato fa riferimento alla predisposizione di un insieme di esempi che vengono proposti alla macchina durante il processo di addestramento.

Di questi esempi si conoscono già caratteristiche e risultato ed è dall'associazione tra i molteplici esempi che la macchina inizia ad imparare comprendendo le relazioni tra richiesta e risultato che può essere conseguito e quindi predisponendosi a conseguire ulteriori risultati originariamente non previsti.

Un esempio pratico può essere di aiuto a comprendere il significato dei dati usati con questo tipo di apprendimento.

Immaginiamo di predisporre un modello di machine learning per prevedere il costo di un viaggio basato su diverse caratteristiche (ad esempio, il numero dei viaggiatori, le stelle dell'albergo, l'ampiezza della stanza).

I dati che verranno raccolti per addestrare il modello comprenderanno quindi gli input (e cioè le caratteristiche del viaggio) mentre l'output consisterà nell'individuazione del risultato che voglio ottenere (e quindi il costo del viaggio) che costituirà la c.d. etichetta.

Nella pratica accadrà che in un dataset etichettato avrò un caso o più casi di cui conosco l'input (domanda) e l'output (risposta) ed il modello userà questi dati per imparare la relazione tra domanda e risposta.

Nell'esempio che abbiamo ipotizzato il sistema di IA avrà un dataset predisposto in cui l'input saranno le caratteristiche del viaggio (es. viaggio per 1 o 2 persone; 3 o 4 o 5 stelle; stanza di tot metri quadrati) mentre il prezzo costituirà l'output quindi l'etichetta che in questo caso io conosco.

La macchina di IA imparerà a fare previsioni sui prezzi dei viaggi sulla base delle caratteristiche che gli vengono fornite dall'utente.

## APPRENDIMENTO NON SUPERVISIONATO (UNSUPERVISED LEARNING)

Va da sé che la spiegazione del sistema alternativo di apprendimento non **supervisionato non può che fare riferimento all'uso di dati NON etichettat**i.

Se nel precedente esempio noi conoscevamo tutte le componenti del modello, in questa ipotesi potrei conoscere sì le caratteristiche del viaggio (quante persone) ma non anche il prezzo corrispondente ad ognuno dei viaggi per cui la procedura si svolgerebbe senza che la macchina sia in grado di reperire l'etichetta di riferimento e che l'avrebbe aiutato nell'elaborare il risultato richiesto (cioè il prezzo).

In questo caso la macchina non potrà quindi fare previsioni ma potrà comunque identificare relazioni (viaggio per 2 persone in albergo a 5 stelle)

### APPRENDIMENTO PER RINFORZO (REINFORCEMENT LEARNING)

Altro sistema di addestramento fa invece riferimento ad un agente (e cioè un programma o un robot) che apprende come prendere decisioni in un certo contesto. Ad ogni sua azione viene associato un premio (se il risultato è giusto) o una penalità (se esso è sbagliato) con l'intento di istruire il sistema al conseguimento di un numero di premi sempre maggiore ed un numero di penalità sempre inferiore.

Questa modalità viene applicata tradizionalmente nei videogames.

Il robot deve cioè eseguire una serie di azioni. L'azione che da un punto all'utente è un premio, l'errore è una penalità.

### FASI DEL PROCESSO DI APPRENDIMENTO AUTOMATICO

A prescindere dalle scelte di una delle tecniche illustrate, il processo di apprendimento automatico generalmente segue questi passi:

- **Raccolta dei dat**i: raccolta cioè di un set di dati che rappresenti il problema che si vuole risolvere.
- **Pre-elaborazione dei dat**i: pulire dei dati, rimuovere i valori mancanti o quelli che non servono a realizzare l'obiettivo.
- **Divisione** dei dati tra quelli che serviranno per l'addestramento e quelli che serviranno per provare il funzionamento del sistema.
- **Scelta del modello**: supervisionato, non supervisionato, per rinforzo.
- **Addestramento del modello**: si usano cioè i dati per insegnare al modello a fare previsioni.
- **Valutazione del modello**: (set di test) si propongono cioè dati che in precedenza il sistema non conosceva al fine di percepire le sue reazioni ed i risultati.
- **Ottimizzazione**: se il test da esito positivo si cerca di migliorarlo.
- **Implementazione**: il sistema viene applicato nel contesto in cui è destinato ad operare (contesto giuridico, contesto sanitario, contesto produttivo etc.).

## 11. APPLICAZIONI DELL'INTELLIGENZA ARTIFICIALE

Lo sviluppo delle procedure che abbiamo esaminato in precedenza aiutano a comprendere l'ampissima area in cui l'intelligenza artificiale può trovare applicazione e che spaziano dal contesto sanitario a quello giuridico, all'industria ed al commercio.

UNIVERSITÀ DEGLI STUDI “MAGNA GRAECIA DI CATANZARO”
Corso di INFORMATICA GIURIDICA
DOCENTE: Avv. Prof. FABRIZIO SIGILLÒ - A.A. 2026/2027

INTRODUZIONE ALLA CONOSCENZA DELL’INTELLIGENZA ARTIFICIALE

## L'INTELLIGENZA ARTIFICIALE NEL SETTORE GIURIDICO

Posizione al primo posto il settore giuridico perché è quello che più attiene al corso di informatica giuridica.

Al netto della iconica visione che si ha dell'IA nel campo giuridico (quella del computer che produce sentenze automaticamente) può dirsi che il diritto sia destinato a risentire positivamente in punto di automazione di compiti ripetitivi quali la stesura e la revisione di contratti tipici dell'attività forense, la gestione di documenti di uso comune nell'attività giuridica e, soprattutto, l'analisi giuridica del caso e cioè la rapida individuazione di un argomento specifico e la proposizione (sulla base delle istruzioni eseguite preventivamente) di soluzioni che si attagliano ad esso.

È chiaro che questi sistemi funzioneranno bene e si riveleranno utili se la fase di istruzione del sistema di IA viene svolta adeguatamente. Se sono quindi corrette le regole dell'istruzione e la macchina riceverà dati giuridici corretti ed affidabili ed allora l'operazione di calcolo si risolverà in pochi attimi.

Adottare questa procedura non significa affidare automaticamente alla macchina una decisione perché quella risposta dovrà essere elaborata ed analizzata dall'uomo che costituisce quindi parte integrante dei cc.dd. sistemi predittivi che vengono applicati proprio in ambito giuridico.

Il sistema predittivo si fonda sulla disponibilità di un set di dati (dataset) quanto mai ampio, fornito da sentenze o da pezzi di sentenze idonee a ricostruire l'esatta associazione tra un fatto e un altro, verificare la decisione assunta in quel frangente e dunque proporre una soluzione. Purtroppo nello sviluppo di questo procedimento, teoricamente impeccabile, interferiscono

## GLI ERRORI DEL SISTEMA DI INTELLIGENZA ARTIFICIALE

suscettibili di rendere non impeccabili i risultati della giustizia predittiva e che sono riconducibili al margine di errore in cui la macchina può incorrere nella fase dell'istruzione o in quella dell'esecuzione.

Già accertate le fattispecie denominate

### ALLUCINAZIONI

ovverosia risposte false o non coerenti generate dalla macchina.

La spiegazione tecnica della causa con cui questo fenomeno si realizza è tradizionalmente ricondotta all'uso, nei modelli di linguaggio come GPT di pattern statistici e cioè degli schemi che prevedono le risposte più probabili ma non anche la loro correttezza.

Le allucinazioni possono altresì discendere da un'errata o incompleta fase di addestramento incompleti.

Ne consegue, in questi casi, che la macchina di IA non reperisca la risposta coerente ma la elabori autonomamente estraendo dall'insieme degli schemi che le sono stati forniti nella fase dell'istruzione, una risposta plausibile ma che non è detto che sia corretta.

L'esigenza che l'istruzione sia quindi quanto più completa possibile si manifesta più sensibilmente nella fase di formazione di strumenti specialistici (diritto, sanità, ingegneristica) necessitanti di una conoscenza specifica.

Determinante un adeguato meccanismo di verifica che renda cioè possibile, nella fase di test, la distinzione tra risposte corrette e allucinazioni.

La macchina, in particolare, può restare pericolosamente vittima del c.d.

BIAS

termine che può intendersi come una distorsione dei dati resi da un sistema di intelligenza artificiale realizzato per l'adozione di una decisione o di una previsione.

Questa tipologia di errore trova un suo precedente proprio nel contesto giudiziario ed in una fattispecie verificatasi negli Stati Uniti.

Un giudice, chiamato a decidere sulla responsabilità di una persona e a quantificare la condanna, si è servito in via esclusiva di un sistema di IA istruito mediante un algoritmo chiamato COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) usato in alcuni tribunali americani usano per determinare il rischio di recidiva dei condannati (il rischio, cioè, che lo stesso soggetto compia lo stesso reato nel corso del tempo).

L'analisi della fase di istruzione del sistema ha consentito di rivelare che i dati impostati con quell'algoritmo erano viziati dall'origine perché presupponevano che fosse più probabile che l'uomo di colore nero reiterasse quel tipo di reato rispetto ad un uomo di colore bianco.

Ovvio l'effetto che ne è conseguito. La macchina ha ritenuto che l'uomo sol perché di colore nero fosse più propenso a commettere nuovamente lo stesso reato, assumendo una decisione evidentemente errata perché basata su una discriminazione fondata su "pregiudizi storici" (es. lo zingaro ruba più spesso degli altri) e che in un sistema che si autoaggiorna automaticamente non può che essere accentuata, perché produttivo di un numero X di decisioni sbagliate.

Altrettanto chiaro che questo problema abbia rivelato la sua pericolosità in quanto applicato in un contesto - quello giuridico - in cui la decisione deve essere improntata a criteri di neutralità e imparzialità. Ma altrettanto evidente che esso debba ritenersi altrettanto pericoloso anche in quegli altri contesti come quelli del mondo del lavoro in cui un algoritmo del genere potrebbe ritenere meno affidabile per un posto di lavoro la donna perché suscettibile di maggiori assenze rispetto all'uomo prima dopo e durante la gravidanza).

# RIDURRE ED ELIMINARE IL BIAS?

È pressoché scontato che l'intervento preordinato a ridurre o eliminare gli errori del bias debba svolgersi nella fase di formazione del sistema, usando dati equilibrati e quanto più possibile vari perché rappresentativi di tutte le categorie di persone.

Non meno importante sarà la fase di test e sua applicazione pratica che, se adeguatamente monitorati, potranno favorire l'individuazione e la correzione dell'algoritmo.

Entrambe queste fasi non possono prescindere dal rispetto dei principi di trasparenza e responsabilità di chi produce i sistemi di IA e di chi li distribuisce; problema questo di non sempre facile applicazione in relazione alla segretezza che copre le idee industriali su cui si fondano i sistemi di IA.

# LA GESTIONE E LA TUTELA DEI DATI PERSONALI

Inevitabile che una gestione così ampia di dati personali debba essere improntata, in tutte le sue fasi (e quindi progettazione, istruzione, utilizzo), al pieno rispetto della normativa vigente in Europa (GDPR) e negli altri stati sul loro trattamento.

Il problema involge certamente il profilo giuridico ma anche e soprattutto quello sanitario destinato cioè ad operare in un contesto di dati particolari come quelli biometrici o, per l'appunto, legati a singole e specifiche patologie od anche in quello finanziario. Scontato ritenere che questo problema sia accentuato dal fatto che il loro trattamento venga gestito mediante gestioni automatizzate.

Base del rispetto delle regole è quindi, in prima battuta, la preventiva informativa da fornire al titolare dei dati personali (come e perché i dati vengono trattati, possibilità di accesso, correzione e cancellazione).

Si unisce l'obbligo di garantire il principio di minimizzazione evitando cioè che l'IA acquisisca, gestisca e rielabori un numero di dati sproporzionati rispetto allo scopo e non quelli effettivamente necessari.

Con esso anche quello di **anonimizzazione** o **pseudonimizzazione** utili a rendere i dati non immediatamente identificabili o a rimuovere completamente l'identificabilità dei dati (sostituendo ad esempio il numero ad un fascicolo piuttosto che il nome dell'interessato e associandolo tra loro in maniera riservata)

In questo contesto si collocano le disposizioni del GDPR europeo che abbiamo già conosciuto nel corso di queste lezioni e che impongono la pratica applicazione della c.d. privacy by design e by default da attuarsi nel processo di sviluppo e nell'architettura dei sistemi IA e nella fase di acquisizione e gestione del dato.

Fondamentale l'attuazione di una corretta DPIA (Valutazione d'Impatto sulla Protezione dei Dati) che, soprattutto in ambito giuridico e sanitario permetta di impostare il comportamento di chi tratta i dati al livello di delicatezza **dei dati trattati.**

## L'INTELLIGENZA ARTIFICIALE NEL SETTORE SANITARIO

Il calcolo in precedenza descritto che associa il fatto agli effetti e propone soluzioni spiega il supporto dell'IA nell'ambito sanitario in cui essa può essere utilizzata per l'analisi di immagini mediche (radiografie, ecografie e risonanze magnetiche) al fine di identificare malattie e anomalie ma anche per la previsione di evoluzione o aggravamento di alcune patologie.

Meno personalizzata ma pur sempre assoggettata alla verifica del professionista è la proposizione di piani terapeutici basati sui dati del paziente e rapportata ad analoghe fattispecie memorizzate nei dati dell'IA.

Inevitabile, attesa la delicatezza di questo contesto, il contributo dell'uomo che deve astenersi dall'applicazione incondizionata delle proposte offerte dall'IA, e mirare al rispetto dei diritti del paziente ed il rispetto delle normative sanitarie, della disciplina professionale e delle convinzioni etiche.

## L'INTELLIGENZA ARTIFICIALE NEL SETTORE LAVORATIVO

Nel campo lavorativo l'IA può spiegare il suo supporto nelle varie fasi del rapporto e quindi:

- ricerca e scelta del personale
- assunzione
- svolgimento dell'attività produttiva
- risoluzione o patologie del rapporto di lavoro

Si è già detto, parlando del BIAS, di come gli errori dell'algoritmo possano influenzare negativamente la selezione del dipendente che affidi ad un sistema di IA la valutazione dei profili personali e dei curricula dei candidati.

Può darsi per scontato, anche perché ampiamente testato ed applicato nel contesto industriale, che una macchina può impattare positivamente sui termini di automazione del lavoro.

Ci si intende riferire, in questo caso, sia al contesto amministrativo (si pensi al sistema di IA che risponde automaticamente attraverso semplici chatbot disponibili su un sito internet di una azienda od anche di una pubblica amministrazione).

Ultimo, ma non ultimo, l'intervento dei robot già da tempo utilizzati nel processo industriale e che affidano alla macchina l'esecuzione (anche completa) di tutte le fasi di costruzione di un apparato.

Questo ultimo profilo costituisce il primario aspetto critico dell'IA nel contesto lavorativo perché neanche tanto teoricamente ispirato ad una riduzione dei posti di lavoro soprattutto nel settore industriale.

# 12. ALTRI SETTORI

## AMBITO FINANZIARIO

L'IA viene in questo caso utilizzata per analizzare grandi volumi di dati in tempo reale e prendere decisioni di sviluppo del mercato finanziario suggerendo soluzioni di investimento (in questo caso il rischio di attività fraudolente non può escludersi se non si conosce il produttore del sistema di IA e i dati che questi ha utilizzato nella fase di istruzione).

## MARKETING E COMMERCIO

È questo un contesto che conosciamo già da tempo grazie ai contributi gratuiti che ci pervengono dalle offerte dei colossi come Google, Amazon o simili che raccolgono e analizzano i dati dei consumatori, offrendo esperienze di acquisto personalizzate e sono in grado di farlo anche in maniera automatica sulla base delle richieste rivolte dall'utente, delle ricerche da questi svolte o degli acquisti effettuati.

## MOBILITÀ

In questo ambito non è del tutto nuova la presenza (ancora prevalentemente a livello sperimentale) dei c.d. veicoli a guida autonoma che evidentemente utilizzano l'IA per prendere decisioni in tempo reale sulla guida, sui percorsi ma anche sulle scelte che garantiscano la sicurezza.

## I RAPPORTI UMANI

Lo sviluppo delle applicazioni di intelligenza artificiale si risolve anche in nuove modalità di gestione dei rapporti sociali, investendo anche le più tradizionali cognizioni che, sul piano etico, caratterizzano alcuni di questi rapporti.

Si è detto degli effetti che la procedura di automazione può produrre sulle attività lavorative e sulla neanche ipotetica riduzione dell'apporto umano, foriera di nuove situazioni di disoccupazione di massa.

Si pensi ancora a interventi mirati a realizzare processi decisionali senza che si conosca però la modalità con cui si provvede - o si è provveduto - ad istruire il sistema artificiale.

Si tratta di problematiche che non possono svilupparsi senza il preventivo contributo giuridico che, così come accaduto con il CAD per la regolamentazione degli strumenti informatici nella pubblica amministrazione, definisca limiti ed estensioni dell'utilizzo dei sistemi di intelligenza artificiale e dei relativi servizi.

# 13. LE ESPERIENZE GIURIDICHE SULL'INTELLIGENZA ARTIFICIALE NEI VARI PAESI

In mancanza di una legislazione globale unificata può farsi riferimento ai tentativi esperiti in alcune parti del mondo ed a quelle realizzate in Europa e, specificamente in Italia.

## STATI UNITI

Non esiste una legge federale specifica sull'IA, ma ci sono diverse iniziative legislative statali. Ad esempio lo stato della California ha approvato il California Consumer Privacy Act, che richiede alle aziende di informare i consumatori sull'uso dei dati personali nelle applicazioni di IA.

## CINA

Già introdotte una serie di leggi e regolamenti sull'IA sin dal 2017. Il governo centrale ha pubblicato un documento che mira a costruire un'industria nazionale dell'IA entro il 2030 e sta anche sviluppando leggi per regolamentare i settori specifici, come la sorveglianza e la sicurezza nazionale.

## CANADA

È stato adottato il "Principio dell'intelligenza artificiale: guida per amministratori pubblici" nel 2020 che individua una sorta di guida etica e legale per l'utilizzo responsabile dell'IA nel settore pubblico.

## REGNO UNITO

La questione dell'IA è stata affidata ad una Authority appositamente creata e determinata Digital Government Ethics (Ada Lovelace Institute). Essa esiste ed opera dal 2018 con l'obiettivo di sviluppare e promuovere buone pratiche etiche nell'utilizzo dell'IA.

## UNIONE EUROPEA

Più vicina alla nostra realtà è l'attività sviluppatasi nell'Unione Europea e già consolidatasi nella proposta di regolamento sulla "legge sull'intelligenza artificiale" (European Artificial Intelligence Act) presentata dalla Commissione europea nel 2021 e confluita nell'atto con cui, il 21 maggio 2024 il Consiglio dell'UE ha comunicato di avere approvato il relativo regolamento.

**Integrazione: dall'AI Act "proposta" all'AI Act "vigente".** La dispensa descrive l'AI Act come proposta del 2021. Oggi il **Regolamento (UE) 2024/1689** è stato pubblicato in GUUE il 12 luglio 2024, è in vigore dal 1° agosto 2024 ed è applicabile dal 2 agosto 2026, salvo le disposizioni con applicazione differita. Non è più una proposta: è diritto vigente e vincolante per tutti gli Stati membri.

# REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE (AI ACT): PRINCIPI E STRUTTURA

**Integrazione: la classificazione per rischio.** Il principio basilare dell'AI Act non è il divieto generalizzato, ma la **classificazione delle applicazioni di IA in base al rischio** e la loro conseguente regolamentazione giuridica. La piramide è composta da quattro livelli:

1. **Pratiche vietate (art. 5).** Manipolazione subliminale o ingannevole, sfruttamento di vulnerabilità, social scoring, identificazione biometrica remota "in tempo reale" in spazi pubblici per finalità di contrasto (con limitate eccezioni). Sono vietate in assoluto.
2. **Sistemi ad alto rischio (art. 6 e Allegato III).** Comprendono, tra gli altri: biometria, infrastrutture critiche, istruzione, occupazione, accesso a servizi essenziali, contrasto alla criminalità, migrazioni, amministrazione della giustizia, processi democratici. Per questi sistemi scattano obblighi rafforzati: gestione del rischio, qualità dei dati, documentazione tecnica, sorveglianza umana, valutazione di conformità.
3. **Sistemi con obblighi di trasparenza (art. 50).** Ad esempio i chatbot, che devono dichiarare all'utente di essere un sistema di IA.
4. **Sistemi a rischio minimo.** Nessun obbligo specifico oltre a quelli generali.

## FRIA (Fundamental Rights Impact Assessment).

L'art. 27 dell'AI Act impone a determinati *deployer* — in particolare soggetti pubblici o privati che erogano servizi pubblici — di svolgere una **valutazione d'impatto sui diritti fondamentali** prima del primo utilizzo di un sistema ad alto rischio. La FRIA deve descrivere: i processi in cui il sistema sarà usato; il periodo e la frequenza d'uso; le categorie di persone potenzialmente colpite; i rischi specifici di danno; le misure di sorveglianza umana; le misure da adottare se i rischi si materializzano. Non va confusa con la **DPIA** del GDPR: la DPIA guarda ai dati personali, la FRIA ai diritti fondamentali in senso ampio. Possono essere coordinate, ma non sono la stessa cosa.

## LE SANZIONI EUROPEE.

L'art. 99 dell'AI Act fissa soglie massime dissuasive: fino a **35 milioni di euro o al 7% del fatturato mondiale annuo** per le pratiche vietate; fino a **15 milioni o al 3%** per la violazione degli altri obblighi (fornitori, deployer, trasparenza); fino a **7,5 milioni o all'1%** per informazioni inesatte alle autorità. Attenzione: sono **massimali**, non importi automatici. Gli Stati membri devono introdurre sanzioni efficaci, proporzionate e dissuasive nel proprio ordinamento.

## OBBLIGHI DI PROVIDER E DEPLOYER.

L'AI Act distingue tra provider (fornitore: chi sviluppa o immette sul mercato il sistema) e deployer (utilizzatore professionale: chi usa il sistema nell'esercizio della propria attività). Gli obblighi del provider sono più intensi (progettazione, conformità, marcatura CE).

Quelli del deployer riguardano l'uso conforme, la sorveglianza umana, l'informazione e, per i sistemi ad alto rischio, la FRIA. Nel settore pubblico, la PA è tipicamente deployer.

### REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (GDPR)

Anche in questo caso scontata l'osservanza delle disposizioni sulla protezione dei dati personali nell'ambito dell'uso dell'IA ed il rispetto di quei principi di compliance con il GDPR in termini di minimizzazione dei dati, trasparenza, informativa, ancor più sentiti rispetto all'ordinario sistema del regolamento europeo privacy in quanto non più affidato al rispetto dei concetti da parte del titolare del trattamento dei dati, ma a procedure decisionali automatizzate.

### DIRETTIVA SULLA RESPONSABILITÀ PER DANNI CAUSATI DA IA (AI LIABILITY DIRECTIVE)

Così come una macchina può causare danni per errori di progettazione, altrettanto può capitare per una macchina che automaticamente fa ed automaticamente prende decisioni. È da questo concetto che si sviluppa la Direttiva sulla responsabilità per danni causati da **IA (AI Liability Directive)** che mira a contemperare le diverse connotazioni giuridiche dei paesi che fanno parte della Comunità europea, tenendo a punto di riferimento l'innegabile rischio che l'IA possa cagionare un danno, in tal senso assicurando la realizzazione del diritto della vittima di conseguire il relativo risarcimento ed in misura adeguata all'entità del danno prodotto.

Anche in questo caso la gestione di questo profilo postula l'individuazione del o dei soggetti che possono essere ritenuti responsabili, atteso che alla creazione del sistema automatizzato concorrono numerosi soggetti (il progettista, l'incaricato della formazione del sistema, chi è incaricato della sua realizzazione e, per alcuni versi, chi utilizza il sistema).

Inevitabile ritenere questo percorso complicato anche in relazione alla diversità dei sistemi giuridici coinvolti nella discussione (il diritto italiano piuttosto che spagnolo) non sempre coincidenti e quindi necessitanti di un preliminare intervento che renda univoco l'intero percorso.

## 14. L'APPROCCIO GIURIDICO DELLO STATO ITALIANO ALL'IA

Al netto dell'inevitabile coinvolgimento dell'Italia nel percorso comunitario comune, devono annotarsi politiche in parte autonome ed iniziative personalizzate per affrontare al meglio il futuro caratterizzato dall'uso dell'IA.

In questo senso è stato adottato nel nostro paese una specifica strategia nazionale sull'intelligenza artificiale (che risale al 2021) a cui concorrono le autorità responsabili già preesistenti nel territorio italiano e quindi: Agenzia per l'Italia Digitale (AgID) ed Agenzia per la Cybersicurezza Nazionale (ACN) e che è ispirata alla promozione dell'adozione dell'IA in vari settori, ma con il rispetto dei principi di sicurezza, equità e protezione dei diritti.

La legislazione italiana si è mossa quindi nel rispetto dei principi adottati a livello comunitario, mirando ad una propria normativa varata il 23 aprile 2024 (disegno di legge per l'introduzione di disposizioni e la delega al Governo in materia di intelligenza artificiale) e completata dalla recente applicazione confluita nella

# 15. LEGGE 132/2025

pubblicata in Gazzetta Ufficiale il 25 settembre 2025 ed entrata in vigore il 10 ottobre dello stesso anno.

La legge si inserisce in un contesto in cui l'intelligenza artificiale sta trasformando rapidamente la nostra società: dal lavoro alla sanità, dalla giustizia alla pubblica amministrazione ed è forse per questo che, così come accaduto per il regolamento privacy, l'Italia ha preferito introdurre specificità nel profilo generale definito dal Regolamento comunitario già citato (UE 2024/1689).

La legge si articola in 6 Capi e 28 articoli:

Capo I: Principi e finalità - Capo II: Disposizioni di settore - Capo III: Strategia nazionale e autorità - Capo IV: Tutela utenti e diritto d'autore - Capo V: Disposizioni penali - Capo VI: Disposizioni finanziarie e finali.

## FINALITÀ PRINCIPALI (ART. 1)

Riassume i tre obiettivi fondamentali perseguiti dalla legge e cioè:

a) Promozione dell'uso responsabile dell'IA

Questo principio realizza in concreto il carattere c.d. antropocentrico della legge, ispirato a garantire un utilizzo "corretto, trasparente e responsabile" dell'intelligenza artificiale sin dalla sua fase iniziale (una sorta di quella privacy by default che abbiamo visto tipica del trattamento dei dati personali) assicurando nella fase di produzione di applicazioni di IA il privilegio della persona umana rispetto alla macchina.

L'art. 1, comma 1, della Legge 132/2025 stabilisce che la legge "promuove un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale, volto a coglierne le opportunità. Garantisce la vigilanza sui rischi economici e sociali e sull'impatto sui diritti fondamentali dell'intelligenza artificiale".

Nell'intento di favorire l'innovazione e lo sviluppo economico attraverso l'IA si uniscono regole e divieti a favore verso l'IA come elemento di miglioramento della produttività, sollecitare la nascita di nuove imprese e quindi incrementare la competitività del Paese.

Pur percependo la virtuale utilità dell'IA la legge non trascura di prendere in dovuta considerazione i rischi **economici, sociali e l'impatto sui diritti fondamentali** escludendo che

possa ritenersi eticamente o socialmente accettabile tutto quello che è tecnologicamente possibile.

## RAPPORTO CON IL REGOLAMENTO UE (ART. 1, COMMA 2)

Pur elaborando la linea tracciata dal regolamento europeo si rende necessario consacrare i limiti di questo intervento, chiarendo che la legge debba svilupparsi in conformità al Regolamento UE 2024/1689 di cui non può contraddire i contenuti, non può estendere obblighi aggiuntivi.

Il comma 2 contiene una clausola di conformità: "Le disposizioni della presente legge si interpretano e si applicano conformemente al regolamento (UE) 2024/1689". In caso di dubbio interpretativo, prevale la lettura compatibile con l'AI Act.

## PARTE II - PRINCIPI GENERALI E DEFINIZIONI

### DEFINIZIONI FONDAMENTALI (ART. 2)

Come tipico del nostro sistema giuridico, l'introduzione della legge italiana è dedicata alle definizioni dei termini che poi vengono esposti nel dettaglio.

**Sistema di intelligenza artificiale**: un sistema automatizzato progettato per funzionare con diversi livelli di autonomia e che può generare output come previsioni, contenuti, raccomandazioni o decisioni.

**Dato**: qualsiasi rappresentazione digitale di atti, fatti o informazioni, incluse registrazioni sonore, visive o audiovisive. Questa definizione ampia è importante perché l'IA si "nutre" di dati.

**Modelli** di IA per finalità generali: quei modelli addestrati su grandi quantità di dati che possono essere adattati a molteplici usi (si pensi ChatGPT, per intenderci).

L'articolo 3 stabilisce i principi che devono guidare ricerca, sviluppo e utilizzo dell'IA e, tra essi:

a) Rispetto dei diritti fondamentali e quindi, in prima battuta la Costituzione italiana, il diritto UE.

b) **Principio di trasparenza**. Gli utenti devono essere messi in condizione di sapere che stanno interagendo con un sistema di IA e capire anche in che modo funziona.

c) **Non discriminazione e parità di genere**. L'IA non può dar vita a discriminazioni basate su sesso, età, origine etnica, religione, orientamento sessuale. Il concetto è particolarmente rilevante in relazione al carattere generativo dell'IA che tende ad apprendere dati e quindi anche eventuali pregiudizi dei dati con i quali vengono addestrati.

d) **Sorveglianza e intervento umano**. I sistemi devono rispettare l'autonomia e il potere decisionale dell'uomo, unico elemento che può assumere la decisione finale e può quindi essere soltanto supportato da uno strumento di IA.

e) **Principio democratico**. L'uso dell'IA non può pregiudicare lo svolgimento con metodo democratico della vita istituzionale e politica e non può quindi interferire mediante notizie non veritiere o manipolate.

f) **Cybersicurezza**. I sistemi di IA devono essere sicuri perché in caso contrario si richia la possibilità che i suoi risultati possano essere manipolati o alterati.

g) **Accessibilità**. per persone con disabilità (Art. 3, comma 7) La legge garantisce il pieno accesso all'IA anche alle persone con disabilità, in conformità alla Convenzione ONU sui diritti delle persone con disabilità.

## PRIVACY E PROTEZIONE DATI (ART. 4)

Lo abbiamo ripetuto già più volte che l’uso dell’IA non può trascurare l’esigenza di tutela del dato personale che la legge affronta in relazione a separate fattispecie.

Protezione dei minori

- Per i minori di 14 anni serve il consenso dei genitori
- I minori tra 14 e 18 anni possono dare il consenso da soli, ma le informazioni devono essere facilmente comprensibili

Trattamento dei dati

Vengono richiamati i principi generali propri del regolamento europeo privacy che impongono che nella fase di addestramento e di utilizzo dei sistemi di IA debbano essere garantiti i principi di:

- liceità (conformità alla legge)
- correttezza (non ingannevolezza)
- trasparente (l'utente deve cioè sapere cosa accade ai suoi dati)
- compatibilità con le finalità originarie

Il tutto si deve svolgere con linguaggio chiaro e semplice, evitando cioè termini tecnici incomprensibili o lunghe condizioni contrattuali.

## PARTE III - DISPOSIZIONI SETTORIALI

## SANITÀ E DISABILITÀ (ARTT. 7-10)

In questo settore l'IA deve mirare al miglioramento del sistema sanitario, alla prevenzione delle malattie. Essa può essere utile ad ottenere diagnosi più accurate e cure personalizzate.

In virtù dei principi generali l'IA non può essere utilizzata per selezionare chi ha accesso alle cure (divieto di discriminazione)

La decisione finale resta sempre al medico (principio antropocentrico) che dovrà informare il paziente ha diritto di essere informato sull'uso dell'IA.

Settore specialistico è quello che riguarda la

### RICERCA SCIENTIFICA (ART. 8)

che viene ritenuto di rilevante interesse pubblico ed impone il rispetto di alcuni principi ineludibili.

Prima tra tutti la possibilità di utilizzare dati anche senza il consenso esplicito del paziente ma a patto che detti dati vengano resi anonimi (senza elementi identificativi diretti).

È obbligatoria l'informativa generale sul sito web del titolare e l'obbligo di comunicazione del trattamento al Garante Privacy

### FASCICOLO SANITARIO ELETTRONICO E PIATTAFORMA IA (ART. 10)

Nell'ottica di realizzazione della digitalizzazione dei servizi dell'amministrazione pubblica e tra essi quelli di creazione del fascicolo sanitario viene istituita una piattaforma di intelligenza artificiale gestita dall'AGENAS (Agenzia Nazionale per i Servizi Sanitari Regionali), diretta a supportare i medici con suggerimenti; aiutare nell'assistenza territoriale, facilitare l'accesso ai servizi delle Case della Comunità.

Ovviamente nel rispetto delle regole generali che abbiamo esaminato in apertura, i suggerimenti non possono essere vincolanti, perché deve essere il medico a mantenere piena autonomia decisionale.

## LAVORO

### PRINCIPI GENERALI (ART. 11)

Obiettivi che possono essere perseguire nel contesto del lavoro sono:

il miglioramento delle condizioni di lavoro; la tutela dell'integrità psicofisica dei lavoratori; l'aumento di qualità e produttività delle aziende.

Il tutto deve essere perseguito mediante l'uso di applicazioni sicure e trasparenti, rispettose della dignità umana, restando fermi i già richiamati principi di non discriminazione e l'informativa che il lavoratore deve ricevere.

Viene creato, presso il Ministero del lavoro un

### OSSERVATORIO NAZIONALE (ART. 12)

Che ha il compito di monitorare l'impatto dell'IA sul mercato del lavoro; individuare i settori più interessati e promuovere la formazione di lavoratori e datori di lavoro.

L'adeguata formazione e preparazione consentirà di limitare gli effetti pregiudizievoli dell'ingresso dell'IA nel mondo del lavoro e che potrebbero tradursi nella graduale sicurezza di

alcuni lavori o nella loro trasformazione od anche nella nascita di nuove figure di lavoro al momento neanche prevedibili.

L'ingresso dell'IA impatterà inevitabilmente anche sullo svolgimento delle

### PROFESSIONI INTELLETTUALI (ART. 13)

In tal senso riferendoci ad avvocati, ingegneri, architetti, commercialisti, destinatari di un principio generale che abilita queste tipologie di attività ad usare l'IA solo per finalità strumentali e di supporto ma mai decisionali, dovendo, in questo contesto prevalere il "lavoro intellettuale" del professionista.

Anche al professionista viene imposto l'obbligo di comunicazione al cliente dell'utilizzo di IA nello svolgimento dell'incarico ricevuto e l'obbligatorio rispetto dei profili di semplicità e comprensibilità dell'informazione.

Inevitabile l'interesse della legge anche all'applicazione della IA nella

### PUBBLICA AMMINISTRAZIONE (ART. 14)

Principio generale, in questo caso è che le amministrazioni possano ed anche debbano usare l'IA, nell'ottica di aumentare l'efficienza, ridurre i tempi dei procedimenti e migliorare i servizi ai cittadini.

Anche in questo caso però in queste finalità l'uso di applicazioni di intelligenza artificiale non possono che essere strumentali e di supporto, restando compito esclusivo del funzionario la cura del provvedimento amministrativo e la conseguente responsabilità per la determinazione assunta.

Di fatto l'amministrazione potrà usare l'IA per smistare automaticamente le pratiche edilizie in base alla complessità, ma la decisione finale sulla concessione del permesso deve prenderla sempre un funzionario umano che a sua volta dovrà rispettare il divieto di discriminazione.

Nell'ambito dell'uso di IA nel settore pubblicistico una posizione a parte merita il settore

## GIUSTIZIA (ART. 15)

in cui questa facoltà viene assoggettata a regole estremamente stringenti dedicate ai vari ambiti operativi.

Specifica la posizione del giudice, unico soggetto a cui è affidata ed in via esclusiva l'interpretazione della legge. Sarà il giudice a dover valutare i fatti e le prove che gli vengono sottoposte e sarà lui a dover adottare i provvedimenti.

Carattere più generalista le altre disposizioni che ripropongono i principi già esaminati e quindi la possibilità di utilizzare IA per l'organizzazione dei servizi di giustizia e la semplificazione del lavoro (es. ricerca giurisprudenza) e le attività amministrative.

La peculiarità del settore giustizia impone l'adozione di una normativa specifica, in mancanza della quale l'uso dovrà essere autorizzata dal Ministero della Giustizia ed anche l'esigenza di adeguata e specifica formazione tanto per i magistrati che per il personale amministrativo.

Sempre di natura pubblicistica ma altrettanto specifico è il settore della

## SICUREZZA E DIFESA (ART. 6)

che viene caratterizzato dalla limitazione nell'uso dell'intelligenza artificiale, che non può essere applicata nell'attività:

- di sicurezza nazionale (servizi segreti);
- di cybersicurezza nazionale (sicurezza informatica)
- di difesa (organizzazione delle Forze Armate)
- di polizia per contrastare reati contro la sicurezza nazionale.

All'individuazione dei settori in cui l'IA può agire e dei limiti generici a cui essa è assoggettata fa seguito l'esposizione delle modalità con le quali questi obiettivi potranno essere perseguiti.

È la parte della legge riservata alla

# PARTE IV - GOVERNANCE E STRATEGIA NAZIONALE

L'Italia si dota a tal fine di una cosiddetta Strategia Nazionale destinata ad essere aggiornata almeno ogni due anni.

### STRATEGIA NAZIONALE PER L'IA (ART. 19)

Essa è predisposta dalla Presidenza del Consiglio competente per innovazione tecnologica e transizione digitale in collaborazione con vari Ministeri e contiene una serie di elementi utili allo sviluppo dei progetti.

Rientrano tra queste misure di sostegno alle imprese e eventi di promozione, formazione e diffusione della conoscenza sull'intelligenza artificiale-

Viene costituito un Comitato di coordinamento, presieduto dal Presidente del Consiglio dei Ministri con il compito di coordinare enti, organismi e fondazioni che operano in questo campo.

L'articolo 20 regola le figure istituzionali responsabili del controllo dei vari momenti del progetto

In prima battuta c'è AgID (Agenzia per l'Italia Digitale) a cui spetterà, tra gli altri compiti, quello di promozione innovazione e sviluppo dell'IA.

L'ACN (Agenzia per la Cybersicurezza Nazionale) dovrà invece vigilare sui sistemi di IA, svolgere attività di ispezione e anche sanzione di inosservanza della legge, promuovere il raggiungimento di elevati livelli di sicurezza informatica.

Si aggiungono ad essi rappresentanza della finanza italiana come la Banca d'Italia, la CONSOB e IVASS che si interessano di vigilare i sistemi di IA che operano nel settore finanziario.

Altre autorità che potranno essere coinvolte sono anche il Garante Privacy e l'Autorità per le Comunicazioni (AGCOM).

Determinante al conseguimento dei risultati è poi la predisposizione degli investimenti finanziari che lo Stato promuove sollecitando l'applicazione della robotica nei settori produttivi, il supporto alle piccole imprese per l'implementazione dei sistemi di IA e la creazione di un mercato caratterizzato dalla disponibilità di dati di alta qualità. Idea prevalente è quella di privilegiare soluzioni nazionali nelle procedure di acquisto pubblico scegliendo, ad esempio, società che collocano i dati su datacenter italiani. Sul piano squisitamente monetario l'investimento iniziale è di 1 miliardo di euro.

Una sezione della Legge è infine dedicata alle

# TUTELE E DIRITTO D'AUTORE

Si applica il principio generale che abbiamo conosciuto esaminando il contenuto della Legge sul diritto d'autore (L. 633/42) e cioè che l'opera è protetta dal diritto d'autore se costituisce risultato del lavoro intellettuale dell'autore, anche se creata con l'ausilio dell'IA.

Sulla base di questo presupposto la semplice immagine richiesta all'IA in maniera generica (ad esempio: disegna un cane) non sarà tutelata, laddove nel caso in cui l'opera si completi con un rapporto creativo del suo autore che abbia significativamente introdotto un significativo lavoro intellettuale sarà tutelata (immaginiamo ad esempio all'uso dell'IA per la redazione di una tesi di laurea).

Se c'è un apporto intellettuale significativo dell'autore quello sarà tutelato ma bisogna evitare di scadere nel plagio e nel rispetto del diritto d'autore delle fonti che a dire il vero erano tutelati anche prima della nascita dell'IA.

## TEXT AND DATA MINING (ART. 70-SEPTIES)

Viene regolato l'uso di opere protette per addestrare sistemi di IA stabilendosi che è possibile estrarre testo e dati da opere online solo se l'attività è svolta legittimamente e nel rispetto delle limitazioni eventualmente poste dal titolare dei diritti (in questo caso si può ipotizzare una limitazione all'uso delle opere apposta dal suo autore e con la quale si vieta il loro utilizzo per l'addestramento dell'IA).

Come avvenuto anche nella legge italiana sul trattamento dati, anche la quella dedicata all'IA è caratterizzata da un interesse dedicato alle

# DISPOSIZIONI IN MATERIA PENALE.

Nel sistema di trattamento dati si è assistito ad un ridimensionamento della rilevanza penale realizzata mediante depenalizzazione di alcune fattispecie degradate al rango di sanzioni amministrative, mentre in questo caso si assiste all'introduzione di una

## AGRAVANTE GENERALE (ART. 26, LETT. A)

nel caso in cui il reato è realizzato usando l'IA ed essa **ostacola la difesa oppure aggrava le conseguenze del reato** (si pensi ad un truffatore che usa deepfake (video falsi generati con IA) per ingannare le vittime).

Nuovo il reato di

## DIFFUSIONE ILLECITA DI CONTENUTI IA (ART. 26, LETT. C)

che punisce con la reclusione da 1 a 5 anni la diffusione di immagini, video o voci falsificati con IA, senza consenso della persona ritratta, causandole un danno.

La previsione è tanto grave da essere perseguita o a seguito di querela (la vittima deve denunciare) ma anche d'ufficio qualora la vittima sia un minore, un incapace o una pubblica autorità.

Aggravanti specifiche sono poi riferite all'uso dell'IA per **spionaggio politico**; aggiotaggio (Art. 2637 c.c.) e manipolazione del mercato.

Le idee consacrate nel Regolamento europeo ed integrate (almeno per l’Italia) dai contenuti della L. 132/2026, trovano finalmente completamenti con le disposizioni attuative che mirano a passare dalla grammatica alla pratica.

In questo contesto si colloca il

# D.LGS. 179/2026

**in vigore dal 23 ottobre 2026** ed attuativo della delega contenuta nella Legge 132/2025.

La sua rubrica è esplicita: "Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di poteri delle Autorità nazionali e di utilizzo dell'intelligenza artificiale nella formazione".

**Autorità nazionali.** Il decreto definisce l'assetto italiano per l'attuazione dell'AI Act:

AgID è l'autorità di notifica

**ACN è l'autorità di vigilanza del mercato**. Banca d'Italia, CONSOB e IVASS vigilano sui sistemi ad alto rischio nel settore finanziario.

Il **Garante Privacy** è competente per i sistemi impiegati in contrasto alla criminalità, frontiere, amministrazione della giustizia e processi democratici. È una ripartizione che segue la logica dell'AI Act: ogni autorità vigila sul settore che già conosce, evitando la creazione di un'autorità nuova.

**Sanzioni.** Il decreto prevede un quadro sanzionatorio **graduato e proporzionato**, con limiti massimi **inferiori** a quelli dell'AI Act e con possibilità di misure non pecuniarie per violazioni di scarsa offensività. Questo è un punto giuridicamente delicato: l'AI Act fissa soglie massime, ma gli Stati possono scegliere importi inferiori purché efficaci, proporzionati e dissuasivi. Il legislatore italiano ha optato per una modulazione più mite, coerente con la tradizione sanzionatoria amministrativa nazionale.

**Formazione e professioni (art. 47).** Il decreto interviene sulla formazione continua degli ordini professionali. I corsi devono includere percorsi di alfabetizzazione all'IA articolati su tre profili: **tecnico** (funzionamento, potenzialità e limiti dei sistemi), **giuridico** (disciplina dell'AI Act e norme nazionali di attuazione) e **deontologico** (responsabilità del professionista, obblighi informativi verso il cliente, principio antropocentrico). Per le professioni sanitarie, l'inclusione nei programmi ECM è rimessa a un accordo in Conferenza Stato-Regioni. È una disposizione che parla direttamente agli studenti di giurisprudenza: la competenza sull'IA non è più solo tecnica, è **obbligo formativo regolamentato**.

**Pubblica amministrazione.** Il decreto consente alle amministrazioni di usare l'IA per reclutamento, formazione e innovazione organizzativa, con l'obiettivo di semplificare l'azione amministrativa. Ma ribadisce il principio della Legge 132/2025: l'IA **assiste**, la decisione resta umana, verificabile e imputabile a una persona. La formazione del personale pubblico — alfabetizzazione di base, riqualificazione specialistica, alta formazione per dirigenti — diventa condizione per un uso legittimo dei sistemi.

# GLOSSARIO GIURIDICO MINIMO DELL'IA

A conclusione di questa dispensa che deve ritenersi un tavolo aperto da integrare ogni mese in virtù dell’aggiornamento immancabile che impatta sull’uso dell’IA, si è ritenuto opportuno integrare un breve glossario che aiuti il lettore alla comprensione di quella terminologia non facili da percepire (come lo erano accountability e compliance per il trattamento dati personali), ancor più dove esposti in una lingua che non è la nostra e con la quale non sempre coincide.

Alto rischio (high-risk).

Non deve intendersi quale "sistema pericoloso" in senso assoluto.

Esso significa che il sistema è elencato nell'Allegato III dell'AI Act (o ricade nell'Allegato I come componente di sicurezza di un prodotto) e che, per il settore in cui opera e per il tipo di decisioni che contribuisce a prendere, è idoneo a incidere in modo significativo su salute, sicurezza o diritti fondamentali.

L'elenco comprende, tra gli altri: biometria, infrastrutture critiche, istruzione, occupazione, accesso a servizi essenziali, contrasto alla criminalità, migrazioni, amministrazione della giustizia e processi democratici. La conseguenza giuridica è che per questi sistemi scattano obblighi rafforzati di gestione del rischio, qualità dei dati, documentazione, sorveglianza umana e valutazione di conformità.

Deployer (utilizzatore professionale). È il soggetto che utilizza un sistema di IA nell'esercizio della propria attività, ma non lo immette sul mercato né lo mette in servizio con il proprio nome.

In tal senso è contrapposto al provider (fornitore), che è chi sviluppa il sistema o lo immette sul mercato.

La distinzione è giuridicamente decisiva: gli obblighi del provider sono più intensi (progettazione, conformità, marcatura CE); quelli del deployer riguardano l'uso conforme, la sorveglianza umana, l'informazione e, per i sistemi ad alto rischio.

FRIA (Fundamental Rights Impact Assessment) – Valutazione d'impatto sui diritti fondamentali.

È un adempimento previsto dall'art. 27 dell'AI Act. Prima di utilizzare per la prima volta un sistema di IA ad alto rischio, determinati deployer — in particolare soggetti pubblici o privati che erogano servizi pubblici — devono svolgere una valutazione che descriva: i processi in cui il sistema sarà usato; il periodo e la frequenza d'uso; le categorie di persone e gruppi potenzialmente colpiti; i rischi specifici di danno; le misure di sorveglianza umana; le misure da adottare se i rischi si materializzano.

Si è già detto che essa non va confusa con la **DPIA** del GDPR: hanno finalità e contenuti diversi, anche se la FRIA può richiamare sezioni della DPIA già svolta. In sintesi: la DPIA guarda ai dati personali, la FRIA guarda ai diritti fondamentali in senso ampio.

**Sistemi vietati.** L'art. 5 dell'AI Act elenca **pratiche che non possono essere immesse sul mercato né utilizzate, indipendentemente dal rischio**: manipolazione subliminale o ingannevole, sfruttamento di vulnerabilità, social scoring, identificazione biometrica remota "in tempo reale" in spazi pubblici per finalità di contrasto (con limitate eccezioni), e altre ancora. Sono il livello "zero" della piramide del rischio.

Sorveglianza umana (human oversight). Non è un semplice "controllo umano" generico. È un requisito di progettazione e di uso: il sistema ad alto rischio deve essere costruito e utilizzato

in modo che le persone incaricate possano comprenderne capacità e limiti, monitorarne il funzionamento, riconoscere il rischio di automation bias (la tendenza a fidarsi automaticamente dell'output della macchina), interpretare correttamente gli output e decidere se intervenire o meno. Nell'ordinamento italiano, questo principio è richiamato dalla Legge 132/2025 come principio antropocentrico: la decisione finale resta umana.

**Sanzioni amministrative pecuniarie.** L'AI Act prevede soglie massime elevate (fino a 35 milioni di euro o 7% del fatturato mondiale per le pratiche vietate; fino a 15 milioni o 3% per gli altri obblighi; fino a 7,5 milioni o 1% per informazioni inesatte). Gli Stati membri devono introdurre sanzioni efficaci, proporzionate e dissuasive. **Attenzione**: le soglie europee sono massimi, non automatici. Il legislatore nazionale può prevedere importi inferiori, purché il sistema sanzionatorio resti effettivo.