



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA  
CAMPUS DI CESENA

# **Informatica e diritto**

## **A.A. 2023/2024**

# **La regolazione della produzione e dell'uso di Intelligenza Artificiale**

**Prof. Andrea Amidei**

Dipartimento di Informatica – Scienza e  
Ingegneria

# Le decisioni automatizzate: trasparenza e rischi di discriminazione

Algoritmi: modelli non più basati solo su paradigma logico-deduttivo e deterministico (stessi input, stessi output), ma su modelli predittivi e basati su correlazioni statistiche

- Logiche diverse da quelle umane, difficilmente comprensibili *ex post* e prevedibili *ex ante*
- Discriminazioni e *bias* cognitivi sia a livello di modello di dati, sia a livello di modello di calcolo dell'A.I.
- Attenzione all'**etica dell'algoritmo**



# La spiegabilità e la trasparenza dell'A.I.

- **Spiegabilità:** la proprietà di un sistema di poter dare una spiegazione ad un essere umano in modo soddisfacente (almeno rispondere alla domanda «perché?»)
- **Interpretabilità:** white box (A.I. simbolica) vs. black box (A.I. sub-simbolica) → come posso «aprire» la black box?
- Basta l'**art. 22 del GDPR**?
- Informare l'interessato potrebbe non bastare, e che tipo di informazioni si dovrebbe dare?



# I primi casi italiani in materia di A.I. (?)

## Casi trasferimenti insegnanti (2019)

- Procedura di gestione dei trasferimenti affidata interamente ad un «*meccanismo informatico basato su un algoritmo*» che avrebbe prodotto «*esiti non trasparenti*»
  - → «trasferimenti pazzi», fuori dalla provincia di residenza, senza considerare le circostanze familiari, dando preferenza a soggetti dotati di punteggi inferiori
- Provvedimenti del Ministero dell'Istruzione **annullati**



# I primi casi italiani in materia di A.I. (?)

## Casi trasferimenti insegnanti (2019)

- L'utilizzo di una procedura informatica che conduca direttamente alla decisione finale «*non deve essere stigmatizzata, ma anzi, in linea di massima, incoraggiata*» per i vantaggi che comporta...
- ... ma occorrono due elementi di garanzia: a) «la piena **conoscibilità a monte** del modulo utilizzato e dei criteri applicati» e b) la possibilità per lo *human in command* di svolgere, a valle, «la necessaria verifica di logicità e legittimità della scelta e degli esiti affidati all'algoritmo» (Consiglio di Stato, n. 8472/2019)



# I primi casi italiani in materia di A.I. (?)

## Casi trasferimenti insegnanti (2019)

**Conoscibilità:** deve essere garantita «*in tutti gli aspetti*», dagli autori dell'algoritmo, al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti

→ «**non** può assumere rilievo la **riservatezza** delle imprese produttivi dei meccanismi informatici utilizzati, i quali, ponendo al servizio del potere autoritativo tali strumenti, ne accettano le relative conseguenze in termini di necessaria trasparenza»



# I primi casi italiani in materia di A.I. (?)

## Casi trasferimenti insegnanti (2019)

→ Nel caso in esame, l'algoritmo non è stato utilizzato in modo conforme ai principi di cui sopra: «non è dato comprendere per quale ragione le legittime aspettative di soggetti collocati in una determinata posizione in graduatoria siano andate deluse»

E... «la materia merita un approccio non emotivo ma capace di delineare un **nuovo equilibrio fra uomo e macchina** differenziato per ogni campo di attività», perché, da un lato, la legge è stata concepita in un'epoca in cui si era ancora lontani dalla «rivoluzione tecnologica» e, dall'altro, non sono condivisibili richiami a «scenari orwelliani»...



# I primi casi italiani in materia di A.I. (?)

Sentenza Consiglio di Stato (novembre 2021)

**Non tutto è A.I.** → differenza tra sistemi «tradizionali» a base algoritmica e A.I.

- algoritmo: «*semplicemente una sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato*» → comunque un certo livello di automazione, tale da ridurre l'intervento umano
- A.I.: meccanismi di machine learning; sistema che non si limita ad applicare le regole software e i parametri preimpostati ma elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni sulla base di tali elaborazioni, secondo un processo di apprendimento automatico





# Obblighi in capo a chi?

La «filiera» in materia di A.I. comprende:

- creatore dell'«algoritmo»;
- creatore/costitutore della banca dati o comunque del dataset fornito all'A.I.;
- trainer dell'A.I.;
- creatore del software che incorpora l'algoritmo;
- produttore dell'hardware che incorpora il software che incorpora l'algoritmo;
- distributore del sistema di A.I. o suo importatore;
- utilizzatore del sistema di A.I.



# La regolazione dell'A.I.

«L'IA può essere estremamente utile ... ma può anche risultare dannosa. Tale danno può essere di natura sia materiale (quando incide sulla salute e sulla sicurezza delle persone), sia immateriale (perdita della privacy, restrizioni della libertà di espressione, pregiudizi alla dignità umana o discriminazioni), e può riguardare un'ampia gamma di rischi. Il quadro normativo dovrebbe concentrarsi su come ridurre al minimo i diversi rischi di danno potenziale»

«Tali rischi potrebbero derivare da **difetti nella progettazione** complessiva dei sistemi di IA o dall'**uso di dati senza che ne siano state corrette le distorsioni**»

(Libro Bianco UE, febbraio 2020)



# Il Regolamento UE per un *Artificial Intelligence Act*

21 aprile 2021: proposta di Regolamento UE per un *Artificial Intelligence Act*, volta a stabilire norme armonizzate in materia di produzione e uso di A.I.

N.B.: È ancora formalmente una **proposta**, anche se è stata **approvata dal Parlamento europeo il 13 marzo 2024**

- Norme e **standard** uguali per tutti coloro che producono sistemi di A.I., a seconda della tipologia di sistemi di A.I. che viene in rilievo (rischio)
- Garantire un mercato sicuro e rispettoso dei **diritti fondamentali**



# Il Regolamento UE per un *Artificial Intelligence Act*



## Cosa regola?

«Sistema di A.I.»: un sistema *machine-based* progettato per operare con differenti livelli di autonomia e che può mostrare capacità di adattamento dopo il primo utilizzo e che, per obiettivi impliciti o espliciti, deriva, dagli input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare gli ambienti fisici o virtuali



# Il Regolamento UE per un *Artificial Intelligence Act*



Approccio basato sul **rischio**, sulla possibile incidenza dei sistemi di A.I. sui diritti fondamentali:

- sistemi di A.I. vietati
- sistemi di A.I. ad alto rischio (*high risk*)
  - standard e regole specifiche
- sistemi di A.I. a rischio limitato
- sistemi di A.I. a basso rischio

Norme a parte su *general-purpose A.I. systems*



# Il Regolamento UE per un *Artificial Intelligence Act*

## Sistemi vietati (rischio inaccettabile)

Esempi:

- sistemi di A.I. che usano *«tecniche subliminali che agiscono senza che una persona ne sia consapevole al fine di distorcerne materialmente il comportamento in modo che provochi a tale persona un danno fisico o psicologico»*
- sistemi di A.I. che *«sfruttano le vulnerabilità di uno specifico gruppo di persone»*
- sistemi di A.I. usati dalle autorità pubbliche per *social scoring* delle persone in base al loro comportamento (Cina)
- sistemi di identificazione biometrica in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto (ad esempio, alla criminalità), con alcune eccezioni
- *«giustizia predittiva»*



# Il Regolamento UE per un *Artificial Intelligence Act*

## Sistemi ad alto rischio (*high risk*)

Rischio di danno per la salute o la sicurezza o rischio di impatto negativo sui diritti fondamentali ritenuto elevato, in relazione al loro utilizzo

### Quali sono?

1. quelli che costituiscono prodotti o componenti di prodotti che, ai sensi del diritto UE, già oggi sono assoggettati a norme di *product safety* (es., dispositivi medici)
2. altri appositamente indicati in un elenco allegato al Regolamento e individuati sulla base del rischio concreto di impatto su diritti fondamentali



# Il Regolamento UE per un *Artificial Intelligence Act*

## Sistemi ad alto rischio (*high risk*)

Esempi:

- Dispositivi medici (ad esempio, in diagnostica)
- Settore dei trasporti (ad esempio, veicoli autonomi)
- Credit scoring («*valutare l'affidabilità creditizia*»)
- Sistemi di gestione dei lavoratori e per accesso a lavoro (ad esempio, concorsi)
- Amministrazione della giustizia (ad esempio, sentenza dell'A.I.)

Sono «attività pericolose» (art. 2050 c.c.)? Produrli o usarli?





# Il Regolamento UE per un *Artificial Intelligence Act*

## Sistemi ad alto rischio (*high risk*)

Devono rispettare una serie di requisiti previsti dal Regolamento, tra cui:

- eliminazione o riduzione dei rischi attraverso un'adeguata progettazione e fabbricazione (***risk management system***)
- adeguata progettazione e predisposizione di «*misure di attenuazione*» ***by design*** per i rischi che non possono essere eliminati
- qualità dei **dati di addestramento**: «*pertinenti, rappresentativi, esenti da errori e completi*» + possedere «*proprietà statistiche appropriate*»



# Il Regolamento UE per un *Artificial Intelligence Act*

## Sistemi ad alto rischio (*high risk*)

- progettazione con funzionamento sufficientemente **trasparente** «da consentire agli utenti di interpretare l'output del sistema e utilizzarlo adeguatamente» (istruzioni per l'uso)
- doveri informativi nei confronti dell'utilizzatore
- «**sorveglianza umana**»: misure integrate nel sistema prima della sua immissione in mercato e in ogni fase del suo funzionamento
- «accuratezza» + «robustezza» + «cibersicurezza»
- «sistemi che continuano a imparare» → **misure di attenuazione**



# Il Regolamento UE per un *Artificial Intelligence Act*

## Sistemi ad alto rischio (*high risk*)

Obblighi per:

- produttori dei sistemi *high-risk* (regolazione tecnologia by design)
- procedure di **valutazione della conformità pre- e post-market** + obbligo di **misure correttive**
- fornitori e importatori dei sistemi *high-risk*
- distributori dei sistemi *high-risk*
- utenti dei sistemi *high-risk*

(obblighi di monitoraggio, obbligo di selezione dei nuovi dati di *input*, obbligo di segnalazione...)



# Il Regolamento UE per un *Artificial Intelligence Act*

## Sistemi ad alto rischio (*high risk*)

Obblighi per:

- produttori dei sistemi *high-risk* (regolazione tecnologia by design)
- procedure di **valutazione della conformità pre- e post-market** + obbligo di **misure correttive**
- fornitori e importatori dei sistemi *high-risk*
- distributori dei sistemi *high-risk*
- utenti dei sistemi *high-risk*

(obblighi di monitoraggio, obbligo di selezione dei nuovi dati di *input*, obbligo di segnalazione...)





ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA  
CAMPUS DI CESENA

## **Prof. Andrea Amidei**

### **Informatica e Diritto**

Dipartimento di Informatica - Scienza e Ingegneria

andrea.amidei3@unibo.it

[www.unibo.it](http://www.unibo.it)