UNIVERSITÀ DEGLI STUDI FIRENZE
DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE
DISIT DISTRIBUTED SYSTEMS AND INTERNET TECHNOLOGIES LAB DISTRIBUTED DATA INTELLIGENCE AND TECHNOLOGIES LAB

SNAP4CITY KM4CITY

AI e Big Data in ambito sanitario

Rischi e Tutele

Paolo Nesi, DISIT Lab, UNIFI (paolo.nesi@unifi.it)
DISIT Lab Https://www.disit.org

Resp. DISIT Lab, Snap4City
Membro del CBDAI R-T, IFAB R-ER, PhD-AI, etc.
Referente: EDIH per UNIFI
Docente di

- Big Data Architecture
- System Security and Data privacy

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
THE Tuscany Health Ecosystem

CC BY NC ND
SOME RIGHTS RESERVED

Artificial Intelligence e Big Data vs sanità

- **Digitalizzazione crescente:**
  - dossier sanitari elettronici, dispositivi IoT medici
- **Evoluzione dei sistemi di supporto alle decisioni, DSS**
  - migliorare diagnosi, trattamenti e prevenzione
  - uso dei big data per se e come training per processi di AI
- **protezione dei dati in un settore altamente sensibile**

Vantaggi dell'AI

- **Diagnosi**
  - precoci tramite analisi predittive
  - *In certi contesti* piu' accurate / sensibili di quelle degli operatori
  - Ripetibili, con modelli condivisi a livello internazionale
  - Vanno sempre supervisionate, ovviamente
- **Personalizzazione delle cure basata sui dati dei pazienti**
  - Medicina personalizzata
- **Identificazione di trend epidemiologici in tempo reale**
- **Sviluppo di simulazioni per farmaci in tempi ridotti**
- **Etc.**

Rischi associati all'uso dell'AI e dei Big Data

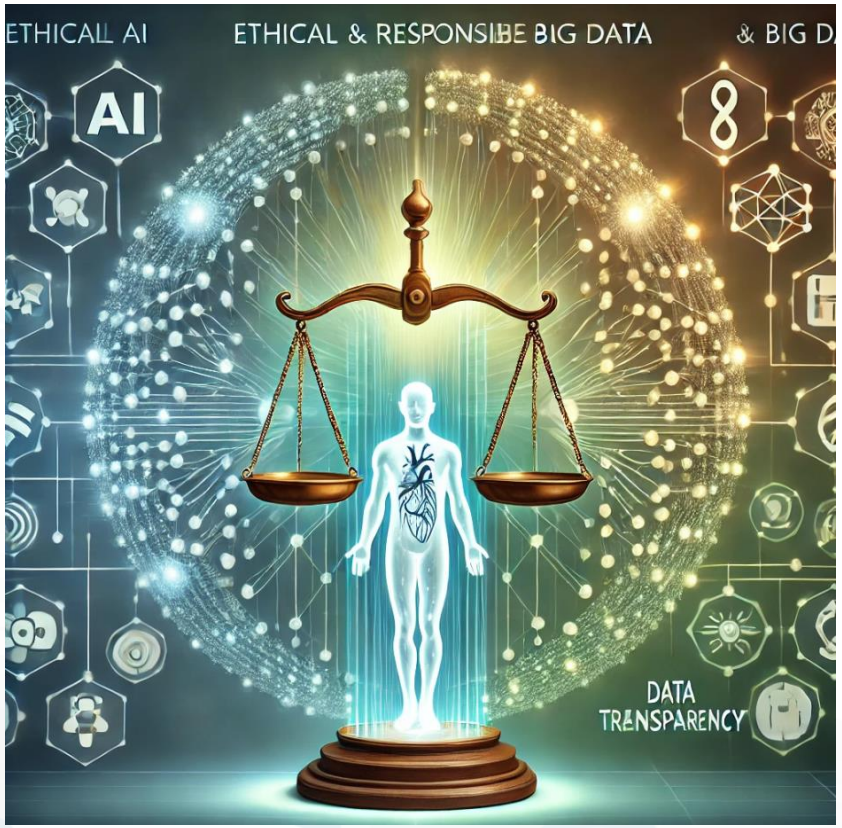
- **Violazione della Privacy:**
  - esposizione di dati sensibili
- **Attacchi:**
  - ransomware, furti di dati
  - Varie tecniche, dall'interno e dall'esterno, sistemi Web esposti
- **Bias algoritmico:**
  - decisioni discriminatorie nei trattamenti sanitari
  - AI-Act e le varie normative dovrebbero aiutare
- **Dipendenza tecnologica:**
  - vulnerabilità delle infrastrutture
  - Open Source

Misure di tutela per un ecosistema sicuro

- **Crittografia avanzata, etc.:**
  - protezione dei dati sensibili, protocolli e formati
  - Certificazione dei dati e loro variazioni
    - blockchain per l'integrità dei dati
- **AI per la sicurezza:**
  - rilevamento di anomalie e attacchi in tempo reale
- **Compliance normativa:**
  - GDPR, AI-Act e regolamenti locali
- **Formazione del personale:**
  - prevenire errori umani

Un uso etico e responsabile di AI e Big Data

- **Necessità di trasparenza negli algoritmi utilizzati**
  - per la trasformazione dati
  - Per i modelli di AI
- **Limitazioni nell'uso dei dati personali per scopi non medici**
  - GDPR (Regulation), AI-Act
- **Collaborazione internazionale per standard comuni**
  - Data Spaces della commissione europea



AI-Act: quadro normativo per l'intelligenza artificiale

- **Obiettivo**
  - Regolamentare l'uso dell'intelligenza artificiale nell'UE per garantire sicurezza ed etica.
- **Rilevanza per la sanità:**
  - Classificazione dei rischi legati agli strumenti AI in base al contesto di uso ed ai dati (basso, medio, alto rischio).
  - Regole rigorose per AI in ambiti ad alto rischio come la diagnosi medica.
- **Impatto**
  - Promuovere la fiducia nell'uso dell'AI proteggendo i dati e i diritti fondamentali.

AI-Act: Impatti specifici sulla sanità

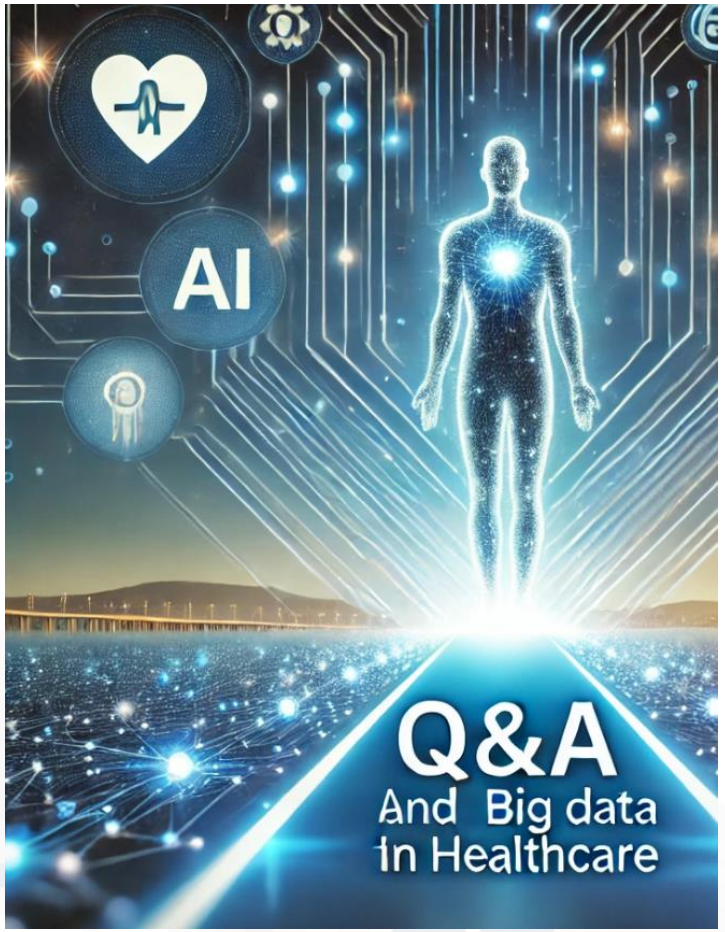
- **Requisiti principali:**
  - Trasparenza e spiegabilità degli algoritmi AI.
  - Sorveglianza continua dei sistemi AI in ambito sanitario.
- **Big Data e privacy:**
  - Protezione dei dati personali e sanitari sensibili.
  - Limitazioni all'uso dei dati per scopi non autorizzati.
- **Implicazioni pratiche:**
  - Necessità di certificazioni per strumenti AI.
  - Maggiore attenzione alle vulnerabilità cybersecurity legate all'uso di AI.

AI-Act, certificazione

- **Procedura di certificazione:**
  - **Valutazione della conformità:** Le aziende devono sottoporre i loro sistemi AI ad alto rischio a una valutazione per verificare il rispetto degli standard previsti. Questa valutazione può essere effettuata attraverso:
    - **Autovalutazione interna:** In alcuni casi, l'azienda può condurre una propria valutazione della conformità.
    - **Valutazione da parte di organismi notificati:** Per determinati sistemi ad alto rischio, è richiesta una valutazione esterna da parte di enti accreditati.
  - **Marcatura CE:** Una volta superata la valutazione, il sistema AI riceve la marcatura CE, indicando la conformità alle normative europee.
- **Obblighi per le aziende:**
  - **Documentazione tecnica:** Mantenere una documentazione dettagliata che descriva il sistema AI, il suo funzionamento e le misure adottate per garantire la conformità.
  - **Gestione del rischio:** Implementare un sistema di gestione del rischio per identificare e mitigare potenziali problemi legati all'uso dell'AI.
  - **Monitoraggio post-mercato:** Sorvegliare continuamente le prestazioni del sistema AI e adottare misure correttive se emergono problemi.
- **Sanzioni per la non conformità:**
  - Le aziende che non rispettano gli obblighi dell'AI Act possono incorrere in sanzioni significative, comprese multe elevate e restrizioni alla commercializzazione dei loro prodotti.

Guardando avanti: Innovazione e protezione

- **XAI, eXplainable AI: AI spiegabile per una maggiore fiducia e motivare i suggerimenti forniti dai sistemi di AI**
  - Sistemi di supporto alle decisioni in ambito sanitario
- **Human in the Loop, Modelli di AI Federata**
  - Sistemi AI che permettono di tenere in considerazione i commenti, suggerimenti dell'utente esperto.
    - Implicazioni sull'evoluzione del modello di AI → ricertificazione
- **Generative AI:**
  - XAI e Human in the Loop ?
- **Evoluzione della Normativa**
  - sulla protezione dei dati sanitari
  - Sulla certificazione del processo e delle soluzioni di AI



Un Caso:

AI a supporto per la valutazione di vertenze medico-legali

- **Analisi del testo** dei documenti relativi al contenzioso, comprensione del linguaggio naturale,
- Per **rispondere a domande** che potrebbero essere quelle da porre ad un esperto che ***studiando il caso*** è in grado di ***rispondere in relazione al contesto*** della singola vertenza. Per esempio
    - *Vi sono altre strutture coinvolte?*
    - *Che tipo di rischio si ha?*
    - *Potrebbe essere conveniente….?*
- **Tecniche**:
    - *Natural Language Processing, BERT, XAI, …*
    - *Modelli Generativi (Generative AI): LLM, Large Language Models: GPT*

Benefici Attesi

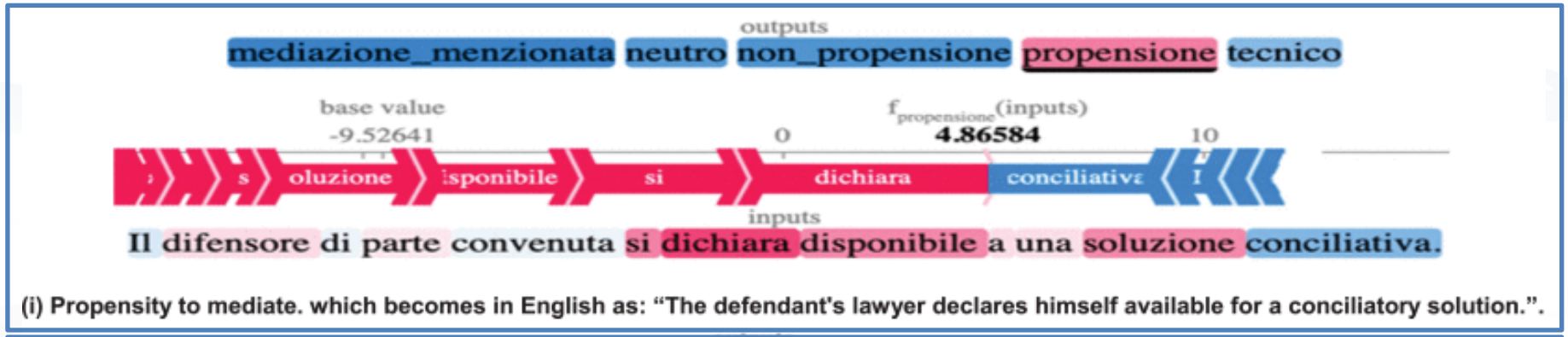
rispondere a domande come un esperto che ***studiando il caso*** è in grado di fornire suggerimenti

- **riferiti** ad affermazioni localizzate nei documenti e fornire spiegazione
- con una **riduzione dei tempi** di analisi di una vertenza,
  - dal punto vista computazionale è instancabile
- **non influenzate** da precedenti documenti,
- **non affetti** da allucinazioni (deduzioni inventate)
- **Con minore varianza** dovuta alle variazioni di contesto, al quale gli umani sono sensibili.

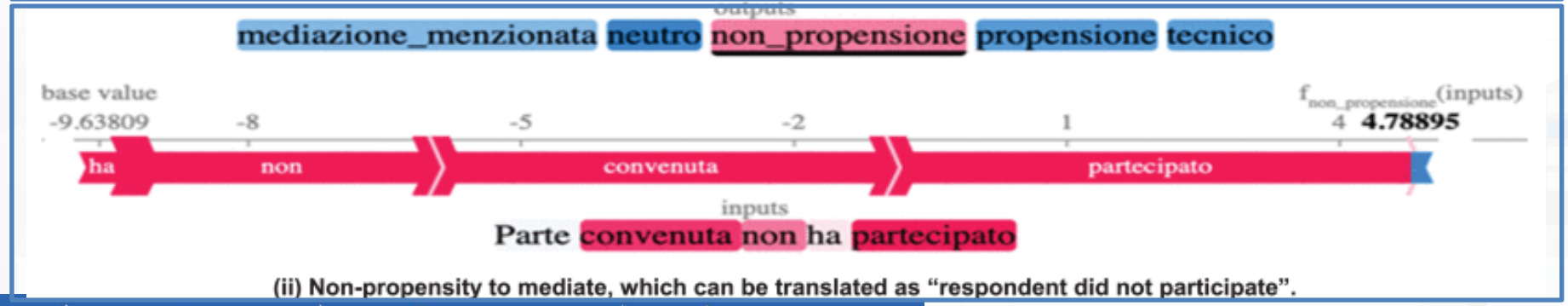
→ ***Decision Support System***

Explainable AI, global/local

- fornire una classificazione ma anche una spiegazione della classificazione delle singole frasi.
- Per questo si utilizzano tecniche di XAI (global e/o local)



(i) Propensity to mediate. which becomes in English as: "The defendant's lawyer declares himself available for a conciliatory solution.".



(ii) Non-propensity to mediate, which can be translated as "respondent did not participate".

Possibile valutare:
Convalidare o Correggere una classificazione

Come vi possiamo aiutare

- Gli aspetti da tenere in considerazione sono moltissimi
- Equilibrio tra innovazione e sicurezza è fondamentale
- Le **univesità e i centri di ricerca sono a disposizione** (delle industrie e delle pubbliche amministrazioni) tramite strumenti come DIH, EDIH, che riducono i costi di accesso, pricinpalmente a
  - Training
  - Procedure di Test Before Invest
- Contratti diretti

AI e Big Data in ambito sanitario

Rischi e Tutele

Paolo Nesi, DISIT Lab, UNIFI (paolo.nesi@unifi.it)
DISIT Lab Https://www.disit.org

CC BY NC ND
SOME RIGHTS RESERVED