Compliance e tutela dei diritti prima ci è scappata di mano la privacy ora ci scapperà di mano l'Intelligenza Artificiale?

di
Riccardo Abeti

Privacy: tante norme, poca protezione
e-privacy XXXV Brescia

Riccardo Abeti

Riccardo svolge la propria attività professionale - tra Milano, Roma e Genova - prevalentemente nelle materie del diritto dell'Information & Communication Technology, Data Protection e Responsabilità amministrativa degli Enti (d.lgs. 231 del 2001).

Dal 1999 presta assistenza legale e organizzativa, coadiuvando le pubbliche amministrazioni clienti nell'elaborazione degli atti suscettibili di incidere sul diritto alla protezione dei dati personali, fornendo pareri, redigendo contratti, linee guida, policy e procedure, conducendo valutazioni di impatto, progettando sistemi di gestione dei flussi informativi (dall'ottimizzazione dei processi esistenti all'implementazione di nuovi processi e procedure) e fornendo attività di docenza nelle materie in cui è specializzato.

- ✓ Presidente della Commissione "New Technology, Personal Data and Communication Law" dell'Unione Avvocati Europei
- ✓ Membro del Comitato esecutivo dell'Unione Avvocati Europei
- ✓ Membro dello CSIG di Ivrea-Torino

di Riccardo Abeti

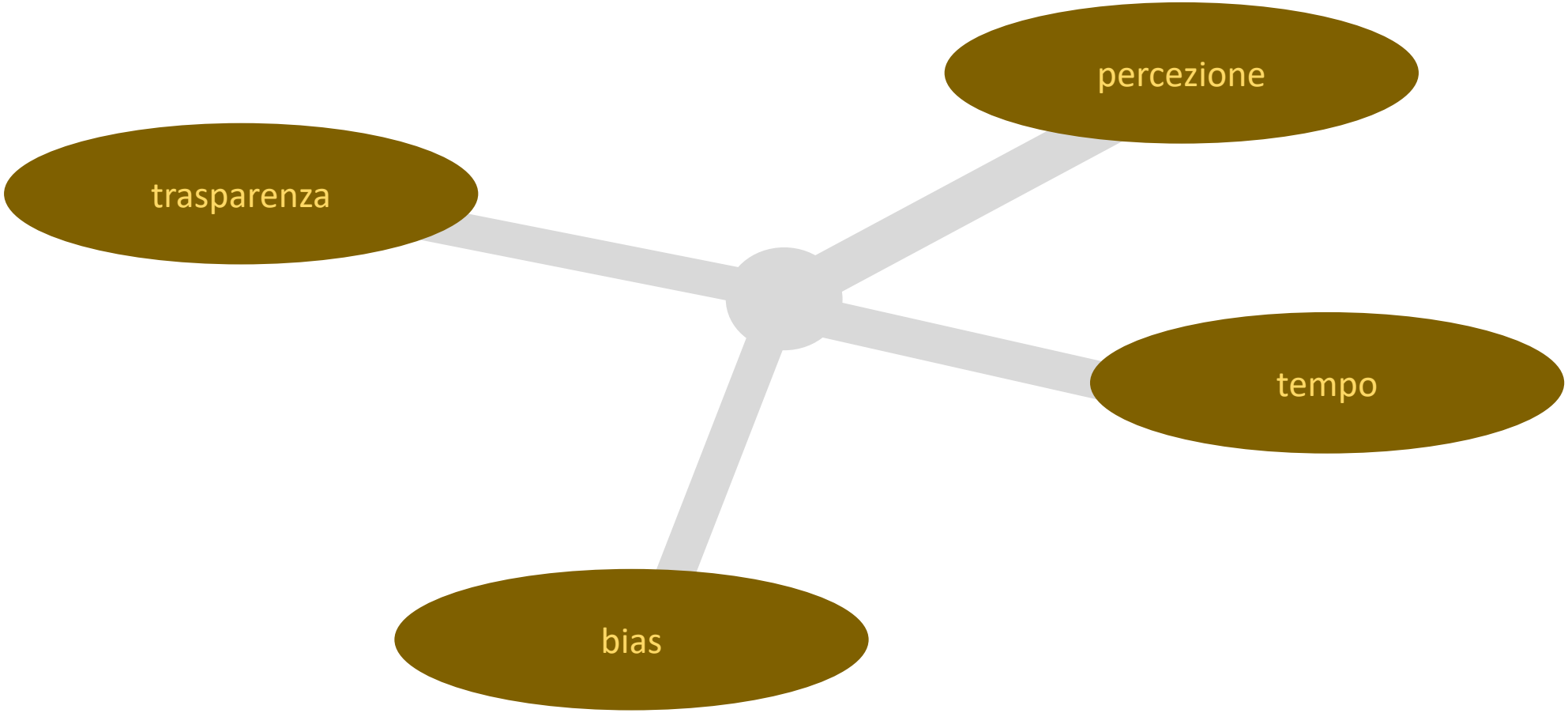
L’intelligenza artificiale non è creativa

L’intelligenza artificiale è solo un motore di ricerca

L’intelligenza artificiale deve essere programmata per non discriminare

L’intelligenza artificiale non ridurrà i posti di lavoro

Questo intervento si articola intorno a quattro elementi



Partiamo da uno dei capisaldi dell'AI ACT:

La trasparenza

1. Comunicazione agli utenti finali 

3. Indicazioni sugli obiettivi e limitazioni del sistema 

2. Trasparenza nel processo decisionale e negli output

4. Tracciabilità dei dati e delle decisioni 

5. Trasparenza nei sistemi di raccomandazione 

1. Comunicazione agli utenti finali

3. Indicazioni sugli obiettivi e limitazioni del sistema

2. Trasparenza nel processo decisionale e negli output

4. Tracciabilità dei dati e delle decisioni

5. Trasparenza nei sistemi di raccomandazione

1. Comunicazione agli utenti finali 

Articolo 52 - Obblighi di trasparenza per determinati sistemi di IA

I fornitori garantiscono che i sistemi di IA destinati a interagire con le persone fisiche siano progettati e sviluppati in modo tale che le persone fisiche siano informate del fatto di stare interagendo con un sistema di IA, a meno che ciò non risulti evidente dalle circostanze e dal contesto di utilizzo. Tale obbligo non si applica ai sistemi di IA autorizzati dalla legge per accertare, prevenire, indagare e perseguire reati, a meno che tali sistemi non siano a disposizione del pubblico per segnalare un reato.

Esempio: **chatbot** e **assistenti vocali** (come descritto nella risposta precedente) devono chiarire la loro natura automatizzata.

 Avete mai avuto un problema serio che un operatore di call center **umano** abbia risolto?

1. Comunicazione agli utenti finali

3. Indicazioni sugli obiettivi e limitazioni del sistema

2. Trasparenza nel processo decisionale e negli output

4. Tracciabilità dei dati e delle decisioni

5. Trasparenza nei sistemi di raccomandazione

2. Trasparenza nel processo decisionale e negli output

Articolo 12 - Conservazione delle registrazioni

I sistemi di IA ad alto rischio sono progettati e sviluppati con capacità che consentono la registrazione automatica degli eventi ("log") durante il loro funzionamento. Tali capacità di registrazione sono conformi a norme riconosciute o a
specifiche comuni.
Le capacità di registrazione garantiscono un livello di tracciabilità del funzionamento del sistema di IA durante tutto il suo ciclo di vita adeguato alla finalità prevista del sistema.

Esempio: **sistemi di valutazione creditizia** o **IA per diagnosi mediche** devono spiegare i fattori chiave delle loro decisioni

di Riccardo Abeti

1. Comunicazione agli utenti finali

3. Indicazioni sugli obiettivi e limitazioni del sistema

2. Trasparenza nel processo decisionale e negli output

4. Tracciabilità dei dati e delle decisioni

5. Trasparenza nei sistemi di raccomandazione

3. Indicazioni sugli obiettivi e limitazioni del sistema

Articolo 13 – Trasparenza e fornitura di informazioni agli utenti

Le informazioni [agli utenti] specificano:

le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio, tra cui:
i) la finalità prevista;
ii) [...];
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;

Esempio: sistemi di IA per la **selezione del personale** o per il **riconoscimento facciale** devono chiarire il contesto e i limiti dei loro utilizzi.

di Riccardo Abeti

1. Comunicazione agli utenti finali

3. Indicazioni sugli obiettivi e limitazioni del sistema

2. Trasparenza nel processo decisionale e negli output

4. Tracciabilità dei dati e delle decisioni

5. Trasparenza nei sistemi di raccomandazione

4. Tracciabilità dei dati e delle decisioni

Articolo 12 – Conservazione delle registrazioni

Le capacità di registrazione garantiscono un livello di tracciabilità del funzionamento del sistema di IA durante tutto il suo ciclo di vita adeguato alla finalità prevista del sistema.

Esempio: **sistemi di giustizia predittiva** o di **valutazione scolastica** devono tenere registrazioni per garantire la tracciabilità delle decisioni.

Un altro concetto che influenza l'AI:

La percezione

Un altro concetto che influenza l'AI:

La percezione

Di chi?

Un altro concetto che influenza l'AI:

La percezione

Di chi?

Degli utenti finali

Dei fruitori

Un altro concetto che influenza l'AI:

L'AI è un business b2c ma soprattutto b2b

La percezione

Degli utenti finali

Di chi?

Dei fruitori

Un altro concetto che influenza l'AI:

L'AI è un business b2c ma soprattutto b2b

La percezione

Cosa vuol dire?

Di chi?

Degli utenti finali

Dei fruitori

Proseguiamo con un fenomeno da non sottovalutare:

La percezione

L'AI è un business b2c ma sopratutto b2b

Vuol dire che se un'azienda implementa un sistema di AI per la selezione del personale e, malgrado i disclaimer, lo usa come se fosse affidabile al 100%, il disclaimer è inutile e i soggetti scartati ne subiscono irrimediabilmente un danno

Degli utenti finali

Dei fruitori

Un altro concetto che influenza l'AI:

L'AI è un business b2c ma soprattutto b2b

La percezione

Cosa vuol dire?

Degli utenti finali

Dei fruitori

Proseguiamo con un fenomeno da non sottovalutare:

L'AI è un business B2C ma soprattutto b2B

La percezione

Vuol dire che se un libero professionista o un consumatore ritiene affidabile un certo strumento e meno costoso della soluzione «umana», lo utilizzerà a dispetto delle *performance*

Degli utenti finali

Dei fruitori

Esempi?

Ho visto pareri scritti dall'AI che facevano riferimento a **norme inesistenti** ma chi mi presentava il parere non lo aveva verificato ...

Il consumatore si accorgerà mai che la dieta è inadatta o che il parere è errato? Che probabilità c'è che se ne accorga?

Se un **sistema di AI consiglia un integratore o una dieta al posto di un dietologo** ma costa molto meno oppure non ha costi apparenti, il consumatore tenderà, specie in assenza di patologie di rilievo, ad affidarsi al sistema di AI **a prescindere dal suo livello di affidabilità certificato** ...

Un altro concetto che influenza l'AI:

bias

bias = *distorsione cognitiva*

Gli algoritmi di apprendimento automatico imparano da grandi *set* di dati.
Cosa accade se tali dati contengono pregiudizi storici o sociali? L'algoritmo li apprenderà e li replicherà.

Ad esempio, se un sistema di AI per la selezione del personale viene addestrato su dati storici in cui determinate posizioni sono occupate da una specifica categoria, potrebbe sviluppare una preferenza per i candidati appartenenti a tale categoria.

Programmatori e sviluppatori possono, involontariamente, immettere i propri pregiudizi nella progettazione e nella realizzazione degli algoritmi.

bias = *distorsione cognitiva*

Ma il motivo per cui faccio cenno al concetto dei **bias** è ulteriore rispetto al fenomeno che è osservato e frutto di studi e tecniche per neutralizzarli.

Analizzando e lavorando ad alcuni progetti di AI ho rilevato che lo stesso tentativo di neutralizzare determinati bias è frutto di un'attività soggettiva e non universale.

Da questa osservazione discende un'ulteriore livello di criticità nell'ambito dello sviluppo dell'AI ovvero una perpetua distorsione dei risultati causata da bias cognitivi e da correzioni che sono anch'esse frutto di posizioni culturali, filosofiche e/o politiche.

di Riccardo Abeti

bias = *distorsione cognitiva*

Analizzando e lavorando ad alcuni progetti di AI ho rilevato che lo stesso tentativo di neutralizzare determinati bias è frutto di un'attività soggettiva e non universale.

Da questa osservazione discende un'ulteriore livello di criticità nell'ambito dello sviluppo dell'AI ovvero una perpetua distorsione dei risultati causata da bias cognitivi e da correzioni che sono anch'esse frutto di posizioni culturali, filosofiche e/o politiche.

Il tempo

la **Legge di Moore** sostiene che la complessità dei microcircuiti, espressa secondo il numero di transistor presenti in un'unità di superficie di un processore di calcolo elettronico (CPU), è in grado di raddoppiare periodicamente.

la **Legge di Moore** sostiene che la complessità dei microcircuiti, espressa secondo il numero di transistor presenti in un'unità di superficie di un processore di calcolo elettronico (CPU), è in grado di raddoppiare periodicamente.

Siamo sicuri che questa legge è ancora valida?

Ad esempio: alla fine del 2019, Google ha affermato di essere riuscita a risolvere in soli 200 secondi un problema che avrebbe richiesto 10.000 anni al supercomputer più veloce del mondo (nel 2019), utilizzando un computer quantistico.

E se introduciamo tra i «motori» dell'evoluzione della capacità di calcolo:

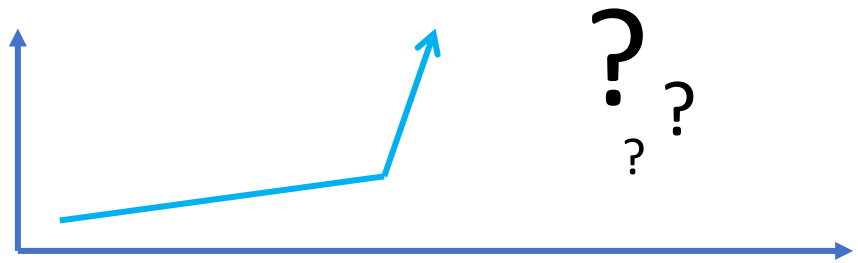
- ❑ la sinergia tra software e hardware?

e

- ❑ la computazione quantistica?

In sostanza il fattore tempo è attualmente calcolato facendo riferimento alla computazione binaria (o alla moltiplicazione dei transistor).

Tuttavia l'applicazione della computazione quantistica può portare a un'evoluzione di tecnologie legate all'AI ben più repentine del previsto, con impatti non sempre prevedibili



Ad esempio: alla fine del 2019, Google ha affermato di essere riuscita a risolvere in soli 200 secondi un problema che avrebbe richiesto 10.000 anni al supercomputer più veloce del mondo (nel 2019), utilizzando un computer quantistico.

Conclusioni

Tenuto conto dei fattori esposti e dei molteplici altri che possono incidere sul tema in oggetto, è lecito pensare che l'approccio dell'AI Act rischi di essere inadeguato al tema che intende regolamentare?

di Riccardo Abeti