

INTELLIGENZA ARTIFICIALE E DIRITTO

# L'AI Act comporta anche l'acquisizione di una cultura digitale di rispetto dei diritti

Oreste Pollicino



Dallo scorso 2 febbraio sono efficaci i primi obblighi previsti dall'AI Act. il riferimento è, da una parte, agli obblighi legati all'utilizzo degli usi vietati, perché considerati dall'Unione europea di un rischio per la tutela dei diritti fondamentali inaccettabile e, dall'altra parte, alla necessità di rendere effettiva una cultura diffusa in tema di AI, la c.d *AI literacy*. Quali i problemi legati all'applicazione, e ancor prima all'interpretazione, di tali obblighi? Con riguardo al divieto di usi proibiti il riferimento è ai sistemi che rappresentano una minaccia diretta ai diritti fondamentali. In particolare sono ora fuori legge i seguenti modelli

1. Manipolazione subliminale – Sistemi che alterano il comportamento delle persone in modo subliminale, compromettendo la loro capacità di prendere decisioni consapevoli e libere
2. Sfruttamento delle vulnerabilità – Tecnologie che approfittano delle vulnerabilità di specifici gruppi di persone, come minori o persone con disabilità, per influenzarne il comportamento in modo dannoso
3. *Social scoring* – Sistemi che classificano le persone in base al loro comportamento sociale o a caratteristiche personali con conseguenze discriminatorie o sproporzionate
4. Riconoscimento biometrico in tempo reale negli spazi pubblici – È vietato l'uso del riconoscimento facciale in tempo reale da parte delle forze dell'ordine, salvo eccezioni per reati gravi come terrorismo o ricerca di persone scomparse
5. Riconoscimento delle emozioni nei luoghi di lavoro e nelle scuole – L'AI Act vieta espressamente l'uso del riconoscimento emotivo in contesti lavorativi e scolastici per

prevenire discriminazioni e invasioni della privacy

6. Uso indiscriminato della categorizzazione biometrica – Sistemi che classificano gli individui in base a dati biometrici o sensibili per finalità che possono violare i diritti fondamentali

Tanti i nodi critici sulla effettiva applicabilità di tali divieti. Qui ci si vuole innanzitutto concentrare su una regolazione complessa relativa sugli usi specifici dell'intelligenza artificiale che pone una netta, e forse parzialmente artificiale distinzione, tra sistemi di riconoscimento biometrico in tempo reale e sistemi ex post. Una distinzione che, oltre a risultare tecnicamente discutibile, genera incertezze normative e operative. Se i primi rientrano nella categoria degli usi vietati, salvo eccezioni dettagliatamente regolamentate, i secondi sono classificati come ad alto rischio. Tuttavia, la differenziazione non incide sulle modalità di autorizzazione, che rimangono nelle mani delle autorità nazionali, sollevando dubbi sulla sua effettiva utilità.

Altra domanda che nasce quasi spontanea. Quali i rimedi in caso di violazione dei diritti in gioco ed in particolare quale il coinvolgimento dell'autorità giurisdizionale quando il regolamento consente un'intrusione nelle sfere più intime della personalità degli individui coinvolti, come nel caso dei processi di riconoscimento fondato su dati biometrici?

A questo proposito va detto che l'AI Act – che rischia di tramutarsi, come in parte è stato per il Gdpr, in una direttiva mascherata per l'altissimo numero di clausole aperte che attribuiscono un significativo margine di manovra agli Stati, lascia a quest'ultimi anche la scelta se ad autorizzare il riconoscimento biometrico sia un'autorità amministrativa o un'autorità giurisdizionale.

La speranza è ovviamente che la scelta degli Stati ricada su quest'ultima opzione, per ovvie ragioni di effettività della protezione dei diritti in gioco e imparzialità dell'organismo di controllo.

Rimane certo l'amaro in bocca pensando che, in un momento in cui l'Unione europea sta affrontando la sfida cruciale dello stato di diritto (anche) al suo interno, non abbia preso una netta posizione a favore dell'unica opzione (quella dell'accertamento giurisdizionale) che, in casi come questi, quando sono in gioco i diritti personalissimi, è la sola conforme alle radici del costituzionalismo europeo.

Passando ora al secondo obbligo a tutti gli effetti entrato in vigore il 2 febbraio, quello legato alla c.d. *AI literacy*, un'altra domanda sembra emergere altrettanto spontaneamente: di cosa effettivamente stiamo parlando?

Potremmo definirla quale quel processo di alfabetizzazione algoritmica che comporta l'obbligo di iniettare una cultura diffusa dell'Intelligenza artificiale. Quindi l'insieme

di competenze cognitive, tecniche e giuridiche necessarie per comprendere, utilizzare in modo consapevole e valutare criticamente i sistemi di Intelligenza artificiale, con particolare attenzione ai loro impatti su diritti fondamentali, accountability e trasparenza.

Questa alfabetizzazione digitale avanzata non si limita alla mera familiarità con il funzionamento delle tecnologie AI, ma include anche la capacità di riconoscere i rischi sistemici connessi ai modelli algoritmici, interpretare il quadro regolatorio europeo e interagire in maniera informata con le dinamiche di governance dell'IA, nel rispetto dei principi di *human oversight* e di *risk-based approach* sanciti dal Regolamento europeo. Affrontare le implicazioni etiche dell'AI, come la tutela della privacy, il rischio di discriminazioni, l'accuratezza delle risposte e le conseguenze per il mercato del lavoro, è il primo passo di un percorso più complesso: la traduzione di questi principi in norme concrete.

Tuttavia, questo processo richiede tempo e il coinvolgimento di molteplici attori, tra cui sviluppatori di tecnologia, utilizzatori e legislatori.

Insomma, al multilateralismo "esterno" necessario per una regolazione condivisa, a livello globale, dell'Intelligenza artificiale si affianca l'esigenza di un pluralismo interno perché tale iniezione di cultura diffusa dell'Intelligenza artificiale in Europa non venga percepita solo come un obbligo, ma anche come grande opportunità.

© RIPRODUZIONE RISERVATA