Intelligenza Artificiale e Regolamentazione: GDPR e AI Act

Alessandro Privitera - Relazione di Educazione Civica e TPS - A.S. 2024/2025

Indice

---

1. Intelligenza Artificiale: definizione e caratteristiche

L'Intelligenza Artificiale (IA) rappresenta una disciplina informatica che mira a sviluppare sistemi in grado di eseguire compiti che normalmente richiederebbero l'intelligenza umana. Si tratta di un insieme di tecnologie che permettono alle macchine di percepire, comprendere, agire e apprendere, sia in modo autonomo che assistito.

L'IA moderna può essere classificata in diversi modi:

- **IA debole o ristretta**: sistemi progettati per svolgere compiti specifici (es. riconoscimento vocale, traduzioni, raccomandazioni personalizzate);
- **IA forte o generale**: sistemi teorici con capacità cognitive simili all'essere umano (attualmente non realizzati);
- **Machine Learning**: sistemi che migliorano attraverso l'esperienza senza essere esplicitamente programmati;
- **Deep Learning**: sottoinsieme del machine learning basato su reti neurali artificiali multistrato.

Le principali caratteristiche dell'IA moderna includono:

- Capacità di elaborare grandi quantità di dati
- Apprendimento automatico da esempi
- Adattamento a nuove situazioni
- Riconoscimento di pattern complessi
- Automazione di processi decisionali

Con l'evoluzione tecnologica, l'IA è diventata una componente fondamentale in numerosi settori: dalla sanità ai trasporti, dall'industria alla finanza, fino ai servizi pubblici. La sua pervasività ha sollevato importanti questioni etiche, giuridiche e sociali, rendendo necessaria una regolamentazione adeguata.

2. Il GDPR e la gestione dei dati personali

Il Regolamento Generale sulla Protezione dei Dati (GDPR - General Data Protection Regulation, Regolamento UE 2016/679) è entrato in vigore nel maggio 2018 e rappresenta il primo significativo intervento legislativo europeo sulla protezione dei dati personali nell'era digitale.

Il GDPR regolamenta la gestione dei dati personali attraverso diversi principi fondamentali:

- **Liceità, correttezza e trasparenza**: i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- **Limitazione della finalità**: i dati devono essere raccolti per finalità determinate, esplicite e legittime;
- **Minimizzazione dei dati**: i dati devono essere adeguati, pertinenti e limitati a quanto necessario;
- **Esattezza**: i dati devono essere esatti e, se necessario, aggiornati;
- **Limitazione della conservazione**: i dati devono essere conservati per un periodo non superiore a quello necessario;
- **Integrità e riservatezza**: i dati devono essere trattati in modo da garantire un'adeguata sicurezza.

In relazione ai sistemi di IA, il GDPR introduce importanti garanzie:

1. **Diritto di non essere sottoposto a decisioni automatizzate**: l'art. 22 stabilisce che l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato che produca effetti giuridici o significativi;
2. **Principio di trasparenza algoritmica**: gli interessati hanno il diritto di ricevere informazioni significative sulla logica utilizzata nei processi decisionali automatizzati;
3. **Valutazione d'impatto sulla protezione dei dati (DPIA)**: obbligatoria per i trattamenti che utilizzano nuove tecnologie e che potrebbero presentare rischi elevati per i diritti e le libertà delle persone;
4. **Privacy by design e by default**: la protezione dei dati deve essere integrata fin dalla progettazione e come impostazione predefinita.

Queste disposizioni, sebbene non specificamente progettate per l'IA, forniscono un primo quadro normativo per affrontare le sfide poste dall'uso crescente di sistemi automatizzati di elaborazione dei dati.

3. AI Act: obiettivi e disposizioni principali

L'AI Act rappresenta il primo quadro normativo completo al mondo specificamente dedicato all'Intelligenza Artificiale. Approvato dal Parlamento Europeo il 13 marzo 2024, entrerà in vigore nel 2025 con un'applicazione graduale fino al 2027.

Gli obiettivi principali dell'AI Act sono:

1. **Garantire che i sistemi di IA immessi sul mercato europeo siano sicuri e rispettino i diritti fondamentali e i valori dell'UE**;
2. **Promuovere gli investimenti e l'innovazione nell'IA in Europa**, creando certezza giuridica;
3. **Migliorare la governance e l'applicazione della normativa esistente** in materia di diritti fondamentali e requisiti di sicurezza;
4. **Facilitare lo sviluppo di un mercato unico per applicazioni di IA legittime, sicure e affidabili**, prevenendo la frammentazione del mercato.

L'approccio adottato dall'AI Act è basato sul rischio, con quattro livelli di regolamentazione:

- **Rischio inaccettabile**: sistemi di IA vietati perché considerati una minaccia per i diritti fondamentali (es. sistemi di scoring sociale, manipolazione cognitiva, identificazione biometrica in tempo reale in spazi pubblici per scopi di polizia salvo eccezioni);
- **Rischio elevato**: sistemi soggetti a rigorosi obblighi prima di poter essere immessi sul mercato (es. sistemi utilizzati in infrastrutture critiche, istruzione, occupazione, servizi pubblici e privati essenziali);
- **Rischio limitato**: sistemi soggetti a specifici obblighi di trasparenza (es. chatbot, sistemi che generano o manipolano contenuti);
- **Rischio minimo**: sistemi soggetti a requisiti minimi o nulli (es. filtri antispam, videogiochi con IA).

Disposizioni particolarmente rilevanti riguardano:

- La regolamentazione dei **sistemi di IA general-purpose** (GPAI) e dei **foundation models** (modelli fondazionali, come i Large Language Models);
- L'istituzione di un **European Artificial Intelligence Board** per garantire un'applicazione armonizzata;
- Un **sistema di governance** con autorità nazionali di vigilanza.

4. Obblighi e requisiti per sviluppatori e utilizzatori

L'AI Act introduce obblighi specifici sia per i fornitori (sviluppatori) che per gli utilizzatori dei sistemi di IA, con particolare attenzione ai sistemi ad alto rischio.

Obblighi per gli sviluppatori:

1. **Sistema di gestione del rischio**: implementare un sistema che identifichi e analizzi i rischi conosciuti e prevedibili, adottando misure appropriate;

2. **Governance dei dati**: garantire che i set di dati di addestramento, convalida e test siano di alta qualità, rilevanti, rappresentativi, privi di errori e completi;
3. **Documentazione tecnica**: mantenere una documentazione dettagliata che dimostri la conformità del sistema;
4. **Registrazione automatica**: garantire che i sistemi registrino automaticamente gli eventi durante il funzionamento;
5. **Trasparenza**: fornire informazioni chiare e adeguate agli utenti sul funzionamento, le capacità e le limitazioni del sistema;
6. **Sorveglianza umana**: implementare misure che consentano una supervisione umana efficace;
7. **Accuratezza, robustezza e sicurezza**: garantire un adeguato livello di precisione, resilienza e protezione da manipolazioni;
8. **Valutazione della conformità**: sottoporsi a procedure di valutazione prima dell'immissione sul mercato;
9. **Registrazione in database UE**: registrare i sistemi ad alto rischio in un database europeo.

Obblighi per gli utilizzatori:

1. **Utilizzo secondo le istruzioni**: seguire le istruzioni d'uso fornite dagli sviluppatori;
2. **Sorveglianza umana**: garantire che persone qualificate supervisionino il funzionamento del sistema;
3. **Monitoraggio**: controllare il funzionamento del sistema per identificare anomalie, malfunzionamenti o prestazioni inattese;
4. **Conservazione dei log**: mantenere i registri generati automaticamente dal sistema;
5. **Valutazione d'impatto**: effettuare una valutazione d'impatto sulla protezione dei dati quando richiesto dal GDPR;
6. **Informativa agli interessati**: informare le persone quando interagiscono con un sistema di IA o quando sono sottoposte a un processo decisionale automatizzato.

Per i sistemi di IA general-purpose e i foundation models, sono previsti obblighi aggiuntivi, come:

- Documentare e analizzare potenziali rischi sistemici;
- Garantire la cybersicurezza e misure per proteggere la proprietà intellettuale;
- Divulgare il contenuto utilizzato per l'addestramento e le politiche di rispetto del copyright;
- Fornire sintesi dettagliate della documentazione tecnica.

5. AI e tutela dei diritti della persona

Le disposizioni relative all'IA contenute nel Regolamento europeo rappresentano una nuova tutela dei diritti della persona e dei propri dati personali, resi maggiormente vulnerabili dalla

pervasività delle nuove tecnologie.

L'AI Act si integra con il GDPR creando un framework completo che affronta le sfide specifiche poste dall'IA:

1. **Protezione della dignità umana**: vietando sistemi che possano manipolare o sfruttare le vulnerabilità delle persone;
2. **Autodeterminazione informativa**: rafforzando il diritto di sapere quando si interagisce con un sistema di IA e come vengono utilizzati i propri dati;
3. **Non discriminazione**: imponendo requisiti di qualità dei dati e test per prevenire bias e risultati discriminatori;
4. **Privacy**: regolamentando in modo rigoroso i sistemi di identificazione biometrica e riconoscimento delle emozioni;
5. **Trasparenza e spiegabilità**: richiedendo che i sistemi di IA ad alto rischio siano comprensibili e tracciabili nelle loro decisioni;
6. **Responsabilità**: stabilendo un chiaro regime di responsabilità per sviluppatori e utilizzatori.

Queste normative riconoscono che nell'era digitale i diritti fondamentali necessitano di nuove protezioni. L'approccio europeo si distingue a livello globale per il tentativo di bilanciare l'innovazione tecnologica con la tutela dei valori fondamentali: l'IA deve servire le persone, non viceversa.

Un aspetto particolarmente innovativo è l'attenzione alla dimensione collettiva della protezione: l'AI Act riconosce che i rischi dell'IA non riguardano solo i singoli individui ma possono avere impatti sociali più ampi, come la polarizzazione dell'informazione o la manipolazione cognitiva di massa.

6. Riflessioni sulle neurotecnologie assistite da IA

Le neurotecnologie assistite da sistemi di IA, che monitorano, sfruttano o influenzano i dati neurali raccolti attraverso interfacce cervello-computer, rappresentano uno degli sviluppi più complessi e delicati nell'ambito delle tecnologie emergenti.

Questi sistemi, in particolare quelli dedicati al riconoscimento delle emozioni, sollevano questioni etiche profonde:

Considerazioni critiche:

1. **Invasione della privacy mentale**: I dati neurali rappresentano il livello più intimo della nostra privacy - i nostri pensieri, emozioni e processi cognitivi. L'accesso a questi dati da parte di sistemi automatizzati solleva interrogativi sul diritto fondamentale alla "privacy cognitiva".
2. **Affidabilità scientifica**: Molti sistemi di riconoscimento delle emozioni si basano su presupposti scientifici non pienamente validati, come l'idea che le emozioni si

manifestino in modo universale e riconoscibile, ignorando le differenze culturali e individuali.
3. **Rischi di manipolazione**: La capacità di rilevare stati emotivi potrebbe essere utilizzata per influenzare comportamenti e decisioni, creando nuove forme di persuasione potenzialmente coercitive.
4. **Discriminazione algoritmica**: Come per altri sistemi di IA, anche le neurotecnologie possono perpetuare bias esistenti, con il rischio di discriminare determinati gruppi di persone in base a come il sistema interpreta le loro risposte neurali.
5. **Autonomia e autodeterminazione**: Il monitoraggio e l'interpretazione continua dei nostri stati mentali potrebbe erodere la nostra capacità di autodeterminazione, creando una forma di "determinismo neurale" che riduce lo spazio per il libero arbitrio.

L'AI Act riconosce questi rischi classificando i sistemi di riconoscimento delle emozioni come sistemi ad alto rischio o, in alcuni contesti, come inaccettabili. Vengono quindi imposti requisiti rigorosi per la loro implementazione, inclusa la trasparenza verso gli utenti e la necessità di sorveglianza umana.

Prospettive personali

Ritengo che le neurotecnologie assistite da IA rappresentino uno dei campi in cui è più necessario un approccio prudenziale basato sul principio di precauzione. Se da un lato queste tecnologie offrono potenzialità straordinarie in ambito medico (come il supporto a persone con disabilità), dall'altro aprono scenari inquietanti quando utilizzate per finalità commerciali, di sorveglianza o di influenza comportamentale.

È fondamentale sviluppare, parallelamente alle tecnologie, nuovi diritti digitali come il "diritto alla privacy cognitiva" e il "diritto all'integrità mentale". La regolamentazione europea rappresenta un primo passo importante, ma sarà necessario un costante aggiornamento normativo per adattarsi all'evoluzione di queste tecnologie.

Un aspetto particolarmente critico riguarda il consenso informato: è realmente possibile comprendere tutte le implicazioni della condivisione dei propri dati neurali? La nostra capacità di esprimere un consenso veramente informato è messa alla prova dalla complessità e dall'opacità di questi sistemi.

In conclusione, credo che lo sviluppo delle neurotecnologie debba essere guidato da un principio fondamentale: il cervello umano e i processi mentali rappresentano il nucleo della nostra identità e autonomia, e meritano la massima protezione possibile. La tecnologia deve rimanere uno strumento al servizio della persona, non un mezzo per la sua manipolazione o controllo.
