

Proposta COM(2021) 206 del 21. Aprile 2021. REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO CHE STABILISCE REGOLE ARMONIZZATE SULL'INTELLIGENZA ARTIFICIALE (LEGGE SULL'INTELLIGENZA ARTIFICIALE) E MODIFICA ALCUNI ATTI LEGISLATIVI DELL'UNIONE

LEGGE EUROPEA SULL'INTELLIGENZA ARTIFICIALE

cepAnalisi 27/2021

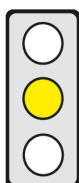
SINTESI [dell'analisi integrale. [Testo completo disponibile in lingua inglese](#)]

Contesto ed obiettivi del regolamento

L'intelligenza artificiale (IA) influenzerà significativamente la vita delle persone in quasi tutti i settori (salute, lavoro, consumo, media, ecc.). Tuttavia, lo sviluppo futuro dell'IA è difficilmente prevedibile oggi. Forme di IA che decidono autonomamente e che auto-apprendono sono in continuo sviluppo e stanno diventando sempre più influenti. Una regolamentazione lungimirante dell'IA, che impedisca applicazioni discriminatorie e manipolative, crei trasparenza e allo stesso tempo permetta l'innovazione è di grande importanza per la sovranità digitale dell'Europa.

Il regolamento mira a creare regole a livello europeo per l'IA, rafforzando così il mercato unico e proteggendo la salute, la sicurezza e i diritti fondamentali degli utenti dell'IA. Adottando un approccio basato sul rischio i sistemi IA particolarmente pericolosi saranno vietati, mentre altri sistemi IA saranno soggetti a: obblighi classificati in base al rischio, codici di condotta volontari o nessun obbligo specifico.

Giudizio sintetico



Pro

- ▶ I requisiti particolarmente rigorosi per i sistemi IA ad alto rischio sono appropriati, poiché questi sistemi di intelligenza artificiale presentano maggiori pericoli.
- ▶ Gli obblighi di trasparenza proposti, anche indipendentemente dal rischio, aumentano l'accettabilità dell'IA da parte della popolazione.

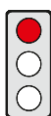
Contro

- ▶ La definizione scelta per identificare i sistemi IA è troppo ampia. Essa dovrebbe comprendere solo i sistemi che imparano e prendono decisioni in modo autonomo.
- ▶ Si deve specificare meglio come i fornitori possano soddisfare i requisiti per i sistemi IA ad alto rischio.
- ▶ Le regole sui sistemi di "punteggio sociale" (*social scoring*) dovrebbero venire estese anche ai fornitori privati.
- ▶ La proposta di regolamento non protegge sufficientemente il diritto alla protezione dei dati.

IA-Definizione

Proposta COM: Un sistema di IA è un software che può produrre risultati - quali contenuti, previsioni, raccomandazioni o decisioni - per obiettivi definiti dall'uomo, influenzando così l'ambiente con il quale interagiamo e che è stato sviluppato utilizzando almeno una delle seguenti tecniche e approcci [Art. 3 (1), Allegato I]:

- Approcci di apprendimento automatico.
- Approcci basati sulla logica e la conoscenza, per esempio la rappresentazione della conoscenza (logica), la programmazione induttiva o i motori inferenziali e deduttivi.
- Approcci statistici, stima bayesiana, metodi di ricerca ed ottimizzazione.



Valutazione del CEP: La definizione dei sistemi di IA data dal Regolamento è troppo ampia. Andrebbe a ricomprendere anche numerose applicazioni software utilizzate già da molti anni che non sono propriamente "intelligenti" ma piuttosto basate sulla logica. La definizione dovrebbe invece considerare prioritariamente se un sistema impara e prende decisioni in modo autonomo.

Ambito di applicazione del Regolamento

Proposta COM: Le disposizioni del Regolamento si applicano a:

- Fornitori di sistemi AI dell'UE e di Paesi terzi che immettono sistemi IA sul mercato dell'UE o li mettono in funzione.
- Utenti commerciali e governativi ("utenti") di sistemi di intelligenza artificiale nell'UE, e
- fornitori e utenti di un Paese terzo quando i risultati generati dai sistemi di IA sono utilizzati nell'UE.

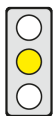


Valutazione del CEP: Il Regolamento crea condizioni di parità per i fornitori UE e non UE. Impedisce anche che il Regolamento venga aggirato implementando sistemi di IA in Paesi terzi per poi utilizzarne i risultati nell'UE.

Sistemi IA ad alto rischio

Proposta COM: I fornitori devono garantire che i sistemi ad alto rischio di IA siano:

- sviluppati con set di dati rappresentativi, privi di errori e completi [Art. 10 (1), (3)];
- sufficientemente trasparenti da permettere agli utenti di interpretare ed utilizzare in modo appropriato i risultati del sistema di IA ad alto rischio [art. 13 (1)];
- sufficientemente accurati, robusti e ciber-sicuri dal punto di vista informatico in relazione allo scopo previsto [Art. 15 (1)].

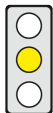


Valutazione del CEP: I requisiti particolarmente rigorosi per i sistemi AI ad alto rischio sono fondamentalmente appropriati, poiché questi sistemi di IA presentano un rischio più elevato. Tuttavia, va specificato come i fornitori possono soddisfare questi requisiti. L'obbligo per i fornitori di garantire l'assenza di errori e la completezza dei dati non può essere soddisfatto.

Obblighi di trasparenza indipendenti dal rischio

Proposta COM: Per i sistemi di IA destinati a interagire con persone fisiche, i fornitori devono garantire che le persone che interagiscono con il sistema di IA siano informate di questo [art. 52 (1)].

Nel caso di sistemi di IA per il riconoscimento delle emozioni o la categorizzazione biometrica - si tratta di sistemi che classificano le persone secondo categorie come età, sesso, origine etnica, orientamento sessuale o politico - gli utilizzatori di tali strumenti devono informare le altre persone interessate riguardo al funzionamento dei sistemi [art. 52 (2)].

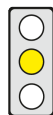


Valutazione del CEP: Gli obblighi di trasparenza proposti, non legati al rischio, aumentano l'accettazione dell'IA da parte del pubblico. Tuttavia, l'uso di sistemi di IA per il riconoscimento delle emozioni o la categorizzazione biometrica dovrebbe essere soggetto a requisiti più rigorosi di un semplice obbligo di informazione.

„socialscoring“

Proposta COM: Le autorità pubbliche non possono utilizzare sistemi di IA che valutano l'affidabilità delle persone fisiche sulla base del loro comportamento sociale o delle loro caratteristiche personali ("social scoring") se questa valutazione portasse a svantaggi per alcune persone, ovvero [art. 5 (1) (c)]:

- in contesti sociali non collegati alle circostanze in cui i dati sono stati originariamente generati o raccolti, o
- in modo ingiustificato o sproporzionato rispetto alla condotta sociale dell'individuo o al suo contesto di vita.



Valutazione del CEP: Le regole sui sistemi di "punteggio sociale" non devono essere applicate solo alle autorità pubbliche, ma anche ai fornitori privati. Perché anche questi - per esempio i social media e i fornitori di servizi *cloud* - possono raccogliere grandi quantità di dati personali ed attuare tecniche di "punteggio sociale" basate su di essi.

Sistemi biometrici di identificazione a distanza

Proposta COM: Un sistema di identificazione biometrica a distanza in tempo reale è un sistema di IA che può identificare a distanza individui sulla base di dati biometrici senza ritardi significativi, e senza sapere in anticipo se l'individuo si troverà in presenza nel contesto di applicazione del sistema di IA [Art. 3 (33) (36), (37)].

L'uso di tali sistemi di identificazione biometrica a distanza in tempo reale in locali accessibili al pubblico e consentito solo per precisi scopi di contrasto al crimine - per altri scopi valgono le regole del GDPR - è quindi consentito solo se è strettamente necessario - tra l'altro, per la ricerca mirata di potenziali vittime di reati [art. (5) (1) (d)].



Valutazione del CEP: L'uso di sistemi di identificazione biometrica a distanza per scopi di polizia interferisce con il diritto alla protezione dei dati (art. 8 CEDU). Il Regolamento ne limita quindi giustamente il loro uso. Tuttavia, non tutela sufficientemente il diritto alla protezione dei dati. In questo contesto, potrebbe non rappresentare una differenza significativa, per le persone coinvolte, se sono identificate in tempo reale o con un ritardo di alcune ore.