SPITCH 1 YEARS

White paper sull'impatto della legge sull'IA dell'UE sull'utilizzo dell'IA conversazionale a fini commerciali

www.spitch.ai

Marzo 2024

Rilevanza e impatto potenziale della legge sull'IA dell'UE per le imprese

Le aziende leader stanno già sfruttando le numerose opportunità offerte da GenAI[1] e LLM[2]. Tuttavia, sono desiderose di trovare un equilibrio tenendo conto degli imperativi di privacy e sicurezza dei dati, anch'essi percepiti come fondamentali dai clienti finali. Le soluzioni di IA conversazionale per il servizio clienti, come gli assistenti virtuali (chatbot testuali e vocali), la biometria vocale e l'analisi vocale, tra le altre fornite da Spitch, fanno davvero la differenza per quanto riguarda le performance di business e la sicurezza dei dati. L'equilibrio tra i vantaggi delle tecnologie innovative, una regolamentazione efficace per controllare i rischi e la responsabilità sociale appare fondamentale per un'adozione sostenibile dell'IA.

L'introduzione della legge europea sull'IA costituisce il primo quadro normativo completo per la governance dell'IA. Essa è destinata ad avere un impatto sia sui fornitori che sugli utilizzatori di alcune forme di GenAI e di biometria a riconoscimento facciale che possono potenzialmente presentare rischi se utilizzate in modo non regolamentato e non controllato. Riteniamo che l'impatto delle nuove normative UE sarà ampiamente positivo per i casi d'uso in diversi settori industriali e nel settore pubblico, con un'influenza relativamente minore sui fornitori di IA conversazionale di specifici domini di business. Tuttavia, tutti i fornitori e gli utenti di sistemi di IA dovranno rispettare alcuni nuovi requisiti.

Si prevede che questi requisiti saranno ulteriormente sviluppati in relazione all'esigenza di standardizzazione alivello europeo. Successivamente, le autorità nazionali dovranno assicurarsi che le imprese si conformino ai nuovi requisiti e standard di governance e gestione del rischio dell'IA, valutando al contempo in che misura possano essere necessarie guide dettagliate per ciascun settore industriale.

Sintesi della legge sull'IA dell'UE*

La legge sull'IA classifica l'IA in base al suo rischio:

- È vietato il rischio inaccettabile (ad esempio, sistemi di punteggio sociale e IA manipolativa).
- La maggior parte del testo riguarda i sistemi di IA ad alto rischio, che sono regolamentati.
- Una sezione più piccola si occupa dei sistemi di IA a rischio limitato, soggetti a obblighi di trasparenza più leggeri: gli sviluppatori e i distributori devono assicurarsi che gli utenti finali siano consapevoli di interagire con l'IA (chatbot e deepfake).
- Il rischio minimo non è regolamentato (compresa la maggior parte delle applicazioni di IA attualmente disponibili sul mercato unico dell'UE, come i videogiochi abilitati all'IA e i filtri antispam – almeno nel 2021; la situazione sta cambiando con l'IA generativa).

La maggior parte degli obblighi ricade sui fornitori (sviluppatori) di sistemi di IA ad alto rischio.

- Chi intende immettere sul mercato o mettere in servizio sistemi di IA ad alto rischio nell'UE, indipendentemente dal fatto che abbia sede nell'UE o in un Paese terzo.
- Sono inclusi anche i fornitori di Paesi terzi in cui l'output del sistema di IA ad alto rischio viene utilizzato nell'UE.

Gli utenti sono persone fisiche o giuridiche che utilizzano un sistema di IA a titolo professionale, non utenti finali interessati.

- **Gli utenti (distributori) di sistemi di IA ad alto rischio** hanno alcuni obblighi, anche se meno dei fornitori (sviluppatori).
- Questo vale per gli utenti con sede nell'UE e per gli utenti di Paesi terzi in cui l'output del sistema di IA viene utilizzato nell'UE.

* Sintesi di alto livello della legge sull'IA

Spitch ritiene che per i clienti e i partner attuali e potenziali possa essere utile esaminare le risposte ad alcune delle domande più frequenti sui nuovi requisiti, riassunte di seguito.

[1] *GenAI - Intelligenza artificiale generativa*

[2] *LLM - Modelli linguistici di grandi dimensioni*

Domande e risposte

1. Quali sono i sistemi di IA vietati ai sensi della legge sull'IA dell'UE? I sistemi di intelligenza artificiale conversazionale per il servizio clienti rientrano nella categoria "vietata"?

I seguenti sistemi di IA sono "vietati" ai sensi della legge sull'IA (Titolo II, Art. 5)[3]:

- Ricorrere **a tecniche subliminali, manipolative o ingannevoli** per distorcere il comportamento e compromettere il processo decisionale informato, causando un danno significativo.
- **Sfruttare le vulnerabilità** legate all'età, alla disabilità o alle condizioni socio-economiche per distorcere il comportamento, causando danni significativi.
- **Sistemi di categorizzazione biometrica** che deducono attributi sensibili (razza, opinioni politiche, appartenenza a sindacati, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale), ad eccezione dell'identificazione o del filtraggio di insiemi di dati biometrici acquisiti legalmente o quando le forze dell'ordine categorizzano i dati biometrici.
- **Classificazione sociale**, ossia la valutazione o la classificazione di individui o gruppi in base al comportamento sociale o a tratti personali, causando un trattamento svantaggioso o sfavorevole di tali persone.
- **Valutare il rischio che un individuo commetta reati penali** basandosi esclusivamente sulla profilazione o sui tratti della personalità, tranne quando viene utilizzato per potenziare le valutazioni basate su fatti oggettivi e verificabili direttamente collegati all'attività criminale.
- **Compilare database di riconoscimento facciale** attraverso il reperimento non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso.
- **Influenzare le emozioni nei luoghi di lavoro o nelle istituzioni scolastiche**, tranne che per motivi medici o di sicurezza.

Sintesi della legge sull'IA dell'UE*

IA per scopi generici (GPAI):

- Tutti i fornitori di modelli GPAI devono fornire la documentazione tecnica, le istruzioni per l'uso, rispettare la direttiva sul copyright e pubblicare una sintesi dei contenuti utilizzati per la formazione.
- I fornitori di modelli GPAI con licenza libera e aperta devono solo rispettare il copyright e pubblicare il riepilogo dei dati di addestramento, a meno che non presentino un rischio sistemico.
- Tutti i fornitori di modelli GPAI che presentano un rischio sistemico - aperti o chiusi - devono inoltre condurre valutazioni dei modelli, test avversari, tracciare e segnalare gli incidenti gravi e garantire le protezioni di sicurezza informatica.

* Sintesi di alto livello della legge sull'IA

* Riassunto di alto livello della legge sull'AI

- **Identificazione biometrica remota (RBI) in tempo reale in spazi accessibili al pubblico per le forze dell'ordine**, tranne che al fine di:
  - Ricercare persone scomparse, vittime di rapimenti e persone vittime della tratta di esseri umani o dello sfruttamento sessuale;
  - Prevenire una minaccia sostanziale e imminente alla vita o un attacco terroristico prevedibile; oppure
  - Identificare i sospetti di reati gravi (ad esempio, omicidio, stupro, rapina a mano armata, traffico di stupefacenti e di armi illegali, crimine organizzato, crimine ambientale, ecc).

Nessuno dei sistemi di intelligenza artificiale conversazionale comunemente utilizzati per scopi commerciali nel servizio clienti rientra in queste categorie.

[3] *Fonte: https://artificialintelligenceact.eu/high-level-summary/*

Molte aziende, in particolare le banche, hanno iniziato a utilizzare la soluzione di verifica dell'identità biometrica vocale in tempo reale per i propri clienti. Nella maggior parte dei casi, serve ad aumentare il processo di verifica dell'identità controllato dall'uomo durante la conversazione in real time con un agente del contact center. Durante la converazione, la voce del cliente viene confrontata con l'impronta vocale precedentemente creata (una rappresentazione matematica delle caratteristiche vocali dell'utente) per assicurarsi che la voce del chiamante corrisponda.

Esistono anche processi di verifica biometrica vocale "ibridi" in cui un numero o una parola generati casualmente vengono ripetuti dal chiamante e la voce dal vivo viene abbinata all'impronta vocale. Questo metodo contribuisce a garantire che la verifica avvenga più rapidamente.

A meno che non siano utilizzati in spazi pubblici dalle forze dell'ordine, questi metodi di autenticazione vocale remota non rientrano nella categoria dei sistemi di intelligenza artificiale vietati.

Tuttavia, se i sistemi di IA conversazionale utilizzano il rilevamento e l'inferenza delle emozioni per informare le decisioni automatiche in un ambiente di lavoro o classificano i chiamanti in base alle emozioni rilevate, tali sistemi possono rientrare nella categoria dei sistemi di IA vietati ai sensi della legge sull'IA dell'UE.

Tuttavia, se l'analisi del sentiment viene utilizzata nell'ambito di un più ampio sistema di intelligenza artificiale del servizio clienti per comprendere il feedback dei clienti e migliorare la qualità del servizio, senza prendere decisioni automatizzate che abbiano un impatto diretto sulle persone, non sarebbe considerato un caso d'uso vietato. È importante sottolineare che la legge sull'IA dell'UE non proibisce l'uso dell'analisi del sentiment in generale, ma piuttosto applicazioni specifiche ritenute ad alto rischio o non etiche. Le aziende devono valutare con attenzione il modo in cui intendono utilizzare l'analisi del sentiment e assicurarsi che non rientri nei casi d'uso vietati delineati dalla legge.

2. Quali sistemi di IA sono classificati come "ad alto rischio" ai sensi della legge sull'IA dell'UE? Esiste la possibilità che l'utilizzo di sistemi di IA conversazionale crei rischi per le aziende a causa di questa classificazione e della necessità di soddisfare requisiti aggiuntivi?

Alcuni sistemi di IA sono considerati "ad alto rischio" ai sensi della legge sull'IA (**Titolo III**)[4]. I fornitori di tali sistemi saranno soggetti a requisiti aggiuntivi. Sistemi di intelligenza artificiale ad alto rischio (**Art. 6**) sono considerati quelli utilizzati come componenti di sicurezza o prodotti coperti dalle leggi dell'UE nell'**allegato II** **E** tenuti a sottoporsi a una valutazione di conformità da parte di terzi ai sensi di tali leggi dell'Allegato II; **o** quelli che rientrano nei casi d'uso dell'**Allegato III** (si veda il riquadro sottostante), tranne se:

- il sistema di intelligenza artificiale esegue un'attività procedurale ristretta;
- migliora il risultato di un'attività umana precedentemente completata;
- rileva modelli decisionali o deviazioni da modelli decisionali precedenti e non intende sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana; oppure
- esegue un'attività preparatoria per una valutazione pertinente ai fini dei casi d'uso elencati nell'Allegato III.

È importante sottolineare che il sistema di IA è sempre considerato ad alto rischio se crea un **profilo delle persone**, ossia se effettua un trattamento automatizzato di dati personali per valutare vari aspetti della vita di una persona, come le prestazioni lavorative, la situazione economica, la salute, le preferenze, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti.

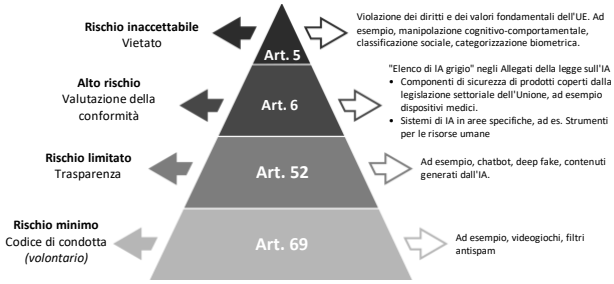
I fornitori che ritengono che il loro sistema di IA, che rientra nell'**Allegato III**, non sia ad alto rischio, **devono documentare** tale valutazione prima di immetterlo sul mercato o metterlo in servizio.

L'articolo 8-25 della legge prevede una serie di requisiti per i fornitori di sistemi di IA ad alto rischio. Tra questi, l'obbligo di istituire un **sistema di gestione del rischio** per tutto il ciclo di vita del sistema di IA ad alto rischio; di condurre un'appropriata **gestione dei dati**, di redigere **documentazione tecnica** per dimostrare la conformità e di fornire alle autorità le informazioni per valutare tale conformità; di garantire che il sistema di IA ad alto rischio preveda la **tenuta di registri**, registrando automaticamente gli eventi pertinenti per l'identificazione dei rischi di livello nazionale e le modifiche sostanziali per tutto il ciclo di vita del sistema.

Altri requisiti includono lo sviluppo di **istruzioni per l'uso** da parte dei distributori a valle per consentire la conformità di questi ultimi e permettere di implementare la **supervisione umana**; garantire gli appropriati livelli di **accuratezza, robustezza e sicurezza informatica**, nonché stabilire un **sistema di gestione della qualità** per assicurare la conformità.

[4] *Fonte: https://artificialintelligenceact.eu/high-level-summary/*

Alcuni sistemi biometrici non vietati, come i sistemi di biometria vocale forniti da Spitch, possono rientrare tra quelli elencati nell'Allegato III. Altri sistemi di IA conversazionale, come chatbot, analisi del parlato, knowledgebase, ecc. possono rientrare nelle categorie "Rischio limitato" o "Rischio minimo", con requisiti aggiuntivi minimi o nulli, come illustrato dal grafico[5] seguente:



3. Qual è la tempistica per garantire la conformità con la legge sull'IA dell'UE?

Spitch offre servizi di consulenza ai propri clienti per contribuire a garantire la piena e tempestiva conformità alle normative, in conformità con la legge sull'IA dell'UE e con gli altri quadri normativi di uno specifico Paese o area geografica, comprese le normative sulla protezione dei dati.

I nostri avvocati aiutano i clienti a formulare i contratti con i clienti sulla base dei requisiti legali esistenti in ogni Paese che regolano la diffusione dei sistemi di IA. Questi devono essere approvati dagli avvocati del cliente prima dell'avvio di qualsiasi progetto.

Di seguito è riportato il grafico[5] che illustra la tempistica di attuazione, secondo la rivista ufficiale dell'UE. Per la maggior parte delle soluzioni di IA conversazionale, ad esempio la biometria e i chatbot non vietati, i requisiti aggiuntivi dovranno essere soddisfatti entro 12-36 mesi a partire dal maggio 2024, quando entrerà in vigore la legge europea sull'IA.

Casi d'uso dell'Allegato III

Biometria non vietata: sistemi di identificazione biometrica a distanza non vietati, esclusi i sistemi di verifica biometrica che confermano che una persona è quella che dice di essere. Sistemi di categorizzazione biometrica che deducono attributi o caratteristiche sensibili o protette. Sistemi di riconoscimento delle emozioni.

Infrastruttura critica: componenti di sicurezza nella gestione e nel funzionamento di infrastrutture digitali critiche, traffico stradale e fornitura di acqua, gas, riscaldamento ed elettricità.

Istruzione e formazione professionale: sistemi di IA che determinano l'accesso, l'ammissione o l'assegnazione a istituti di istruzione e formazione professionale a tutti i livelli. Valutare i risultati dell'apprendimento, compresi quelli utilizzati per guidare il processo di apprendimento dello studente. Valutare il livello di istruzione adeguato per un individuo. Monitorare e rilevare i comportamenti vietati degli studenti durante i test.

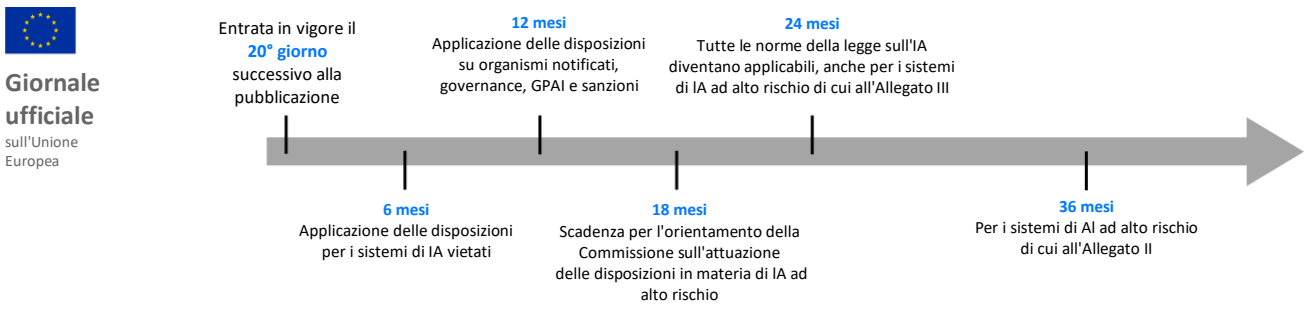
Occupazione, gestione dei lavoratori e accesso al lavoro autonomo: sistemi di IA utilizzati per il reclutamento o la selezione, in particolare annunci di lavoro mirati, analisi e filtraggio delle candidature e valutazione dei candidati. Promozione e risoluzione dei contratti, assegnazione delle attività in base ai tratti della personalità o alle caratteristiche e al comportamento, monitoraggio e valutazione delle prestazioni.

Accesso e fruizione di servizi pubblici e privati essenziali: sistemi di IA utilizzati dalle autorità pubbliche per valutare l'ammissibilità a benefici e servizi, compresa la loro assegnazione, riduzione, revoca o recupero. Valutazione del merito creditizio, ad eccezione dell'individuazione di frodi finanziarie. Valutazione e classificazione delle chiamate di emergenza, compresa la definizione delle priorità di invio di polizia, vigili del fuoco, assistenza medica e servizi di triage per pazienti urgenti. Valutazione del rischio e determinazione dei prezzi nelle assicurazioni malattia e vita.

Applicazione della legge: sistemi di IA utilizzati per valutare il rischio di diventare vittima di un crimine. Poligrafi. Valutazione dell'affidabilità delle prove durante le indagini o i procedimenti penali. La valutazione del rischio di reato o di recidiva di un individuo non si basa esclusivamente sul profilo o sulla valutazione dei tratti della personalità o del comportamento criminale passato. Profilazione durante le indagini, le investigazioni o i procedimenti penali.

Gestione dell'immigrazione, dell'asilo e del controllo delle frontiere: poligrafi. Valutazione della migrazione irregolare o dei rischi per la salute. Esame delle domande di asilo, di visto e di permesso di soggiorno e dei relativi reclami relativi all'ammissibilità. Rilevare, riconoscere o identificare persone, ad eccezione della verifica dei documenti di viaggio.

Amministrazione della giustizia e processi democratici: sistemi di intelligenza artificiale utilizzati nella ricerca e nell'interpretazione dei fatti e nell'applicazione della legge a fatti concreti o utilizzati nella risoluzione alternativa delle controversie. Influenzare i risultati di elezioni e referendum o il comportamento di voto, escludendo i risultati che non interagiscono direttamente con le persone, come gli strumenti utilizzati per organizzare, ottimizzare e strutturare le campagne politiche.



[5] *Fonte: https://www.engage.hoganlovells.com/knowledgeservices/news/the-eu-ai-act-an-impact-analysis-part-1*

4. Ci sono disposizioni della legge sull'IA dell'UE che renderebbero impossibile o troppo rischioso l'utilizzo di soluzioni di intelligenza artificiale conversazionale fornite da Spitch?

In breve, non ce ne sono.

Alcune disposizioni richiederebbero il rispetto di requisiti aggiuntivi da parte del fornitore dei sistemi di IA, cioè Spitch, ma non dei clienti. Spitch garantisce che tutte le soluzioni che utilizzano la biometria vocale in tempo reale, l'analisi del sentiment e il rilevamento delle emozioni, quelle che fanno riferimento a GPT-4 o ad altri modelli di IA per scopi generali per la sintesi e la categorizzazione, nonché i sistemi classificati dalla legge europea sull'IA come "a rischio limitato", come gli assistenti virtuali (chatbot di IA), siano pienamente conformi entro i termini previsti.

5. Quali sono i nuovi obblighi dei clienti che utilizzano i sistemi di intelligenza artificiale forniti da Spitch ai sensi della legge sull'IA dell'UE?

Ai sensi dell'articolo 52 della legge, chi utilizza un sistema di riconoscimento delle emozioni o un sistema di categorizzazione biometrica deve informare le persone fisiche esposte e trattare i dati personali in conformità al regolamento (UE) 2016/679, al regolamento (UE) 2016/1725 e alla direttiva (UE) 2016/280, a seconda dei casi.

Inoltre, chi impiega un sistema di IA che genera o manipola un testo pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico deve dichiarare che il testo è stato generato o manipolato artificialmente.

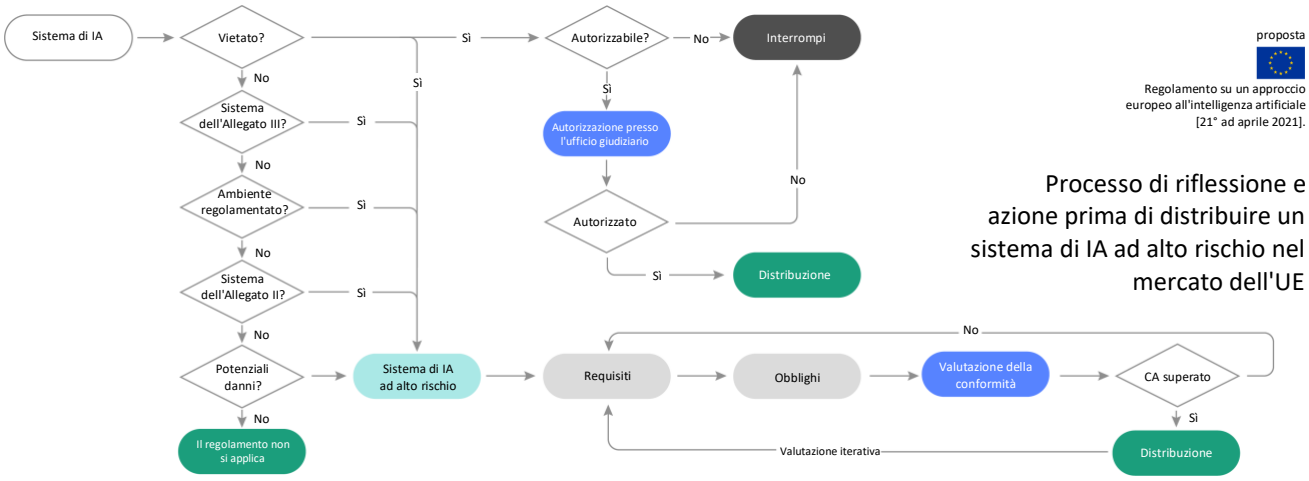
Le informazioni di cui sopra devono essere fornite alle persone fisiche interessate in modo chiaro e distinguibile al più tardi al momento della prima interazione o esposizione. Le informazioni devono rispettare i requisiti di accessibilità applicabili.

Le modalità di implementazione dei requisiti possono variare a seconda della soluzione Spitch; il nostro team di servizi professionali vi assisterà durante l'implementazione per assicurarvi la conformità alle normative più recenti.

6. L'estrazione di dati sulle prestazioni nell'ambiente di lavoro ai fini della gestione della qualità è consentita dalla Legge? Quali azioni garantiscono la legalità?

L'estrazione di tali dati da parte dei sistemi di IA è consentita a meno che non venga utilizzata per prendere decisioni automatizzate senza il coinvolgimento di esseri umani, per dedurre emozioni sul posto di lavoro, per dedurre dati sensibili (razza, opinioni politiche, appartenenza a sindacati, credenze religiose o filosofiche, vita sessuale o orientamento sessuale), o per la classificazione sociale, ossia per valutare o classificare individui o gruppi sulla base di comportamenti sociali o tratti personali, causando un trattamento dannoso o sfavorevole di tali persone.

Per stabilire se le disposizioni del nuovo regolamento si applicano al vostro caso specifico, o nel caso in cui uno dei sistemi di IA possa rientrare nella categoria "ad alto rischio", secondo la legge sull'IA dell'UE, si raccomanda la seguente procedura decisionale[6] per garantire la conformità:



[6] *Fonte: https://futurium.ec.europa.eu/en/european-ai-alliance/open-discussion/more-visual-guide-proposed-eu-artificial-intelligence-act?language=da*