economiesuisse

FAQ sull'intelligenza artificiale IA

L'essenziale in breve:

- L'intelligenza artificiale sta cambiando radicalmente l'economia e la società, ma solleva anche questioni complesse.
- Le nuove FAQ di economiesuisse forniscono risposte e indicazioni su alcune di queste importanti questioni.

L'importanza dell'intelligenza artificiale (IA) per le imprese e la società è in costante aumento. Ma il suo utilizzo dà luogo a numerose questioni legali e pratiche. Insieme all'avvocato Cornelia Stengel e agli avvocati Luca Stäuble e Jonas Tresch, economiesuisse ha redatto delle nuove FAQ. Queste forniscono una panoramica dei principali aspetti normativi e applicativi dell'IA.

Nota legale: questa raccolta ha uno scopo puramente informativo e di sensibilizzazione e non sostituisce la consulenza legale. economiesuisse non si assume alcuna responsabilità per azioni od omissioni in relazione all'uso di queste informazioni.

A completamento e continuazione delle seguenti FAQ,, troverà ulteriori strumenti e informazioni grazie allo strumento di autovalutazione dell'IA e nel blog di Kellerhals Carrard.

FAQ sull’intelligenza artificiale (IA)

1. Come definiamo l’IA?

Il termine «IA» non è facile da definire, per questo motivo non è ancora stata stabilita una descrizione standardizzata. Il Parlamento europeo fornisce una possibile definizione con la seguente formulazione:

«L'intelligenza artificiale è la capacità di una macchina di imitare le abilità umane come il pensiero logico, l'apprendimento, la pianificazione e la creatività».

A differenza dei processi convenzionalmente automatizzati, i casi d'uso dell'IA non sono schemi "se-allora" pre-programmati, ma algoritmi di "apprendimento". Di conseguenza, la maggior parte delle definizioni richiede anche un certo grado di autonomia e un modo per imitare le capacità umane.

2. Quali sono le opportunità dell'IA?

Le applicazioni supportate dall'intelligenza artificiale offrono numerose opportunità. In particolare, possono aumentare significativamente l'efficienza, la produttività, la disponibilità e la qualità (ad esempio, nel contesto del marketing, del servizio clienti o della conformità). A causa delle numerose e sempre nuove aree di applicazione, con l'ulteriore sviluppo tecnico dell'IA emergono costantemente nuovi vantaggi.

3. Quali sono le sfide dell'IA?

Le sfide che sorgono in relazione all'IA non sono solo di natura tecnica, ma toccano anche dimensioni etiche, economiche e legali. In particolare, si tratta dei rischi di protezione dei dati, del rischio di discriminazione, dell'uso di applicazioni basate sull'IA per attività illegali e della frequente mancanza di trasparenza. Queste sfide devono essere sempre tenute in considerazione quando si pianifica l'uso della tecnologia basata sull'IA.

4. Qual è lo stato attuale della regolamentazione dell'IA in Svizzera?

La Svizzera non dispone (ancora) di una normativa specifica per lo sviluppo, la distribuzione o l'utilizzo di applicazioni supportate dall'IA. Ma il Consiglio federale ha incaricato il DATEC di presentare un rapporto entro la fine del 2024, che dovrebbe individuare possibili approcci per la regolamentazione dell'IA. È quindi prevedibile che la regolamentazione dell'IA arrivi anche in Svizzera. Resta da vedere quale forma assumerà questa regolamentazione. Inizialmente è ipotizzabile un approccio "orizzontale" o intersettoriale, come nel caso dell'UE con il regolamento sull'IA ("AI-Act"), entrato in vigore il 1° agosto 2024. Tuttavia, questo approccio non tiene adeguatamente conto delle caratteristiche specifiche del settore e, secondo gli autori, dovrebbe essere respinto. Si dovrebbe invece perseguire un approccio orientato ai risultati, che disciplini solo i casi in cui ciò sia appropriato sulla base di una valutazione preventiva del rischio.

5. Ciò significa che attualmente l'utilizzo dell'IA avviene in un vuoto giuridico?

No. Le norme giuridiche svizzere sono in genere concepite in modo tale da essere applicate indipendentemente dalla tecnologia utilizzata (la cosiddetta “neutralità tecnologica”). Un'azienda che offre ad esempio consulenza sugli investimenti deve rispettare le leggi in materia (ad esempio la legge sulla finanza) anche se esegue l'analisi finanziaria con il supporto dell'IA. Inoltre, anche questioni trasversali come la legge sulla protezione dei dati svolgono un ruolo importante nelle applicazioni dell'IA.

Inoltre, le autorità svizzere (ad esempio la FINMA) pubblicano regolarmente consigli pratici e aiuti all'interpretazione per aumentare la certezza del diritto per le società.

6. A quali disposizioni applicabili occorre prestare particolare attenzione quando si utilizza l'IA?

Nei casi in cui è previsto l'uso di IA generativa (ad esempio, ChatGPT), sorgono diverse questioni relative al copyright. Ad esempio, è importante che lo sviluppatore di tali applicazioni sappia quali dati è autorizzato a utilizzare come dati di addestramento. Questa questione è attualmente all'esame dei tribunali di molti Paesi e resta da vedere se e in che misura si troverà una soluzione standardizzata. Per l'operatore dell'applicazione si pone il problema di quali dati può utilizzare come dati di input, cioè per il “prompt”. Se i dati di input sono opere protette dal diritto d'autore (ad esempio testi o immagini), è generalmente necessaria una licenza. Va inoltre notato che l'output generato dall'IA può anche violare il copyright di terzi. Questo problema è particolarmente rilevante se l'output deve essere reso disponibile a terzi. Infine, si pone la questione se e a quali condizioni l'output generato dall'IA goda della protezione del copyright. La tutela del diritto d'autore richiede una “creazione intellettuale”, che generalmente manca nel caso delle opere generate dall'IA. Sono possibili eccezioni se l'output riflette la creazione intellettuale dell'operatore o semplicemente si aggiunge alla creazione intellettuale di un essere umano (ad esempio nel caso di traduzioni). Altri pareri sono favorevoli all'applicazione del diritto d'autore alle applicazioni di IA a determinate condizioni. Essi sostengono che la creazione intellettuale è presente anche nell'output generato dall'IA (ad esempio, attraverso l'impostazione di parametri). A causa delle incertezze sopra descritte, le questioni devono essere valutate caso per caso, tenendo conto delle circostanze specifiche, e si devono osservare gli ulteriori sviluppi.

Poiché i dati personali vengono regolarmente elaborati anche in relazione all'uso di applicazioni supportate dall'intelligenza artificiale, è necessario prestare particolare attenzione al rispetto della legge sulla protezione dei dati, anche perché la violazione di alcune disposizioni della legge sulla protezione dei dati è (ora) soggetta a sanzioni (ad esempio l'obbligo di fornire informazioni).

Nei casi in cui le applicazioni supportate dall'IA siano fornite da un fornitore di servizi (ad esempio, Software as a Service [SaaS]), tale fornitore di servizi riceva l'accesso ai dati personali ed elabori tali dati per conto del proprio cliente, occorre inoltre garantire che vengano effettuati i necessari chiarimenti in merito alla garanzia della sicurezza dei dati e che vengano presi i necessari accordi contrattuali con il fornitore di servizi (ad esempio, la conclusione di un contratto di elaborazione degli ordini).

Se le applicazioni supportate dall'intelligenza artificiale vengono utilizzate per prendere decisioni (aziendali), occorre verificare in ogni caso se si tratta di una «decisione individuale automatizzata» ai sensi della legge sulla protezione dei dati. Questo è il caso se la decisione si basa esclusivamente sul trattamento automatizzato di dati personali ed è di una certa complessità (ad esempio, la selezione di candidati al lavoro o le decisioni su un credito). L'esistenza di una tale decisione può comportare particolari obblighi di informazione.

In pratica, spesso devono essere osservate ulteriori disposizioni specifiche per il settore, che devono essere identificate prima di tutto in base alle circostanze in cui avviene l'applicazione dell'IA.

7. Come devo procedere se voglio utilizzare un'applicazione di IA?

L'uso di applicazioni AI può portare rapidamente a conseguenze legali. Lo ha dimostrato anche il processo tra il consigliere nazionale dell'UDC Andreas Glarner e la consigliera nazionale Sibel Arslan (Verdi). Andreas Glarner ha pubblicato un video modificato dall'intelligenza artificiale del consigliere nazionale che invitava, tra l'altro, a votare per il consigliere nazionale dell'UDC. La consigliera nazionale Sibel Arslan ha successivamente intrapreso un'azione legale ed ha ottenuto ragione.

Per evitare conseguenze negative, prima di utilizzare un'applicazione di IA è sempre necessario effettuare un'analisi dei rischi. Tra le altre cose, occorre verificare se l'applicazione fornisce risultati affidabili e non discriminatori, se il fornitore dell'applicazione in questione è in grado di garantire la sicurezza dei dati e se i diritti di utilizzo dei dati in entrata e in uscita sono regolamentati. Altri punti da regolare con il fornitore riguardano in particolare la riservatezza dei segreti aziendali e le questioni di responsabilità.

È consigliabile tenere un registro delle applicazioni AI utilizzate in azienda. Questo può includere, ad esempio, le responsabilità interne e le misure (contrattuali) adottate (ad esempio in materia di sicurezza dei dati). Se necessario, tale registro può anche essere integrato in qualsiasi registro esistente sul trattamento dei dati personali ("registro del trattamento").

Infine, occorre verificare se l'utilizzo dell'applicazione AI rientra nell'ambito di applicazione della legge sull'AI. In caso di incertezza sul ruolo della vostra impresa nell'ambito dell'AI Act, visitate lo strumento di autovalutazione dell'IA. La vostra impresa potrebbe essere soggetta a severi requisiti di conformità, soprattutto quando utilizza "sistemi di IA ad alto rischio".

8. Qual è la situazione giuridica nell'UE e in che misura le imprese svizzere sono interessate?

a. Qual è lo scopo e il contenuto normativo dell'EU AI Act?

Con l'AI Act (in vigore dal 1° agosto 2024), l'UE intende promuovere lo sviluppo e l'uso dei sistemi di IA riducendo al minimo i rischi per la salute, la sicurezza e i diritti fondamentali.

L'AI Act adotta un approccio alla regolamentazione dei sistemi di IA basato sul rischio. Il livello di rischio di ogni singolo caso e gli obblighi da rispettare devono essere chiariti nel dettaglio.

L'AI Act distingue di principio le seguenti categorie di rischio:

- Pratiche di IA vietate (ad es. social scoring): tali sistemi di IA non devono essere impiegati.
- Sistemi di IA ad alto rischio: tali sistemi di IA sono soggetti a requisiti specifici come parte di un sistema di gestione del rischio. Gli relativi obblighi si applicano principalmente ai fornitori del sistema di IA. Ma alcuni obblighi si applicano anche agli operatori del sistema.
- Sistemi di IA con rischio limitato: in particolare i sistemi di IA che interagiscono con gli interessati (ad esempio, i chatbot) e i sistemi di IA generativi sono soggetti ad alcuni obblighi di trasparenza.

- Sistemi di IA con rischio minimo: sono esclusi dall'ambito di applicazione della legge sull'IA.

L'AI Act è entrato in vigore il 1° agosto 2024, ma prevede diversi periodi di transizione per l'attuazione dei requisiti: un breve periodo di transizione di sei mesi si applica al regolamento sulle pratiche di IA vietate. I requisiti per i sistemi di IA ad alto rischio devono essere implementati entro 36 mesi. Agli altri requisiti si applica un periodo di 24 mesi.

b. A chi si applica in linea di principio l'AI Act?

L'AI Act riguarda principalmente i fornitori e gli operatori di sistemi di IA. I fornitori sono persone o aziende che sviluppano sistemi di IA e li immettono sul mercato dell'UE; gli operatori sono persone o aziende che utilizzano tali sistemi sotto la propria responsabilità. Il settore personale e non professionale, invece, non è contemplato.

c. L'AI Act si applica anche a persone o imprese in Svizzera?

Come il GDPR, l'AI Act ha un campo di applicazione extraterritoriale. Ciò significa che anche i fornitori e gli operatori di sistemi di IA in Paesi terzi come la Svizzera possono rientrare nel campo di applicazione del regolamento se il sistema di IA in questione viene utilizzato all'interno dell'UE o il risultato ("output") generato dal sistema di IA viene utilizzato all'interno dell'UE.

Le imprese svizzere dovranno verificare caso per caso se esiste un "collegamento" con l'area dell'UE per i sistemi di IA che utilizzano. Visiti in merito lo strumento di autovalutazione dell'IA.

9. Esempio di studio I: Campagna pubblicitaria con l'IA

Sono responsabile della campagna pubblicitaria di un nuovo prodotto e vorrei utilizzare un'applicazione di IA generativa per creare un poster con un'immagine e uno slogan pubblicitario. Cosa devo tenere presente?

In primo luogo, occorre chiarire internamente se esistono linee guida specifiche per l'acquisto e/o l'utilizzo di applicazioni di IA. In caso contrario, il progetto dovrebbe essere colto come un'opportunità per implementare un'adeguata

governance dell'IA in azienda, che includa in particolare la definizione di responsabilità e processi.

Nella scelta del fornitore di servizi per l'applicazione di IA, è necessario tenere in considerazione, tra gli altri, i seguenti punti:

- Il fornitore del servizio concede alla nostra azienda i necessari diritti di proprietà intellettuale o il diritto di utilizzare commercialmente l'output generato dall'applicazione AI (design del cartellone, slogan, ecc.)?
- Se i dati personali (ad esempio dei nostri clienti o collaboratori) sono richiesti come dati di input quando si utilizza l'applicazione AI: il fornitore di servizi garantisce la sicurezza dei dati (riservatezza, integrità e disponibilità dei dati personali in questione) ed esiste un contratto scritto di elaborazione degli ordini (il cosiddetto "ADV") in conformità con la legge applicabile sulla protezione dei dati (LPD e, se applicabile, GDPR)?
- Se i nostri dati aziendali (ad esempio, know-how) sono richiesti come dati di input: il fornitore di servizi garantisce la riservatezza dei nostri segreti aziendali?

Se l'AI Act si applica all'uso dell'applicazione AI (si veda la domanda 8 di cui sopra; ad esempio, perché la campagna è condotta anche nell'UE e l'output è quindi utilizzato nell'UE), si applica quanto segue: se un cartellone coinvolge un contenuto di immagine che è un cosiddetto "deepfake" (cioè materiale di immagine dall'aspetto ingannevolmente reale), deve essere reso noto che questo contenuto è stato creato o manipolato artificialmente. Questa informazione deve essere portata all'attenzione delle persone fisiche interessate (cioè del pubblico nel caso della campagna pubblicitaria) in modo chiaro e riconoscibile al più tardi al momento della prima esposizione.

Per le imprese in Svizzera che non sono soggette all'AI Act, l'attuale legislazione svizzera non prevede l'obbligo esplicito di esporre un avviso corrispondente. Pertanto, se la campagna pubblicitaria è rivolta esclusivamente a persone in Svizzera, l'AI Act non dovrebbe essere applicata. Ma l'IFPDT richiede alle aziende di garantire che l'uso di sistemi che consentono di realizzare deepfakes sia sempre chiaramente riconoscibile dalle persone interessate. Inoltre, l'etichettatura può essere richiesta anche in base alla legge sul commercio equo e solidale.

10. Esempio di caso II: decisioni automatizzate nel processo di reclutamento

Sono responsabile dell'acquisto e dell'introduzione di un sistema di intelligenza artificiale interno che, nell'ambito del nostro processo di reclutamento, effettua una preselezione supportata dall'intelligenza artificiale delle candidature presentate da Germania, Liechtenstein e Svizzera, suggerisce profili adatti e informa i candidati sull'ulteriore processo di reclutamento. Le altre candidature riceveranno automaticamente una decisione negativa. Abbiamo degli obblighi particolari?

Per determinare eventuali obblighi in relazione all'AI Act potenzialmente applicabile, è necessaria la seguente valutazione iniziale: (1) il ruolo della vostra azienda nel contesto dell'applicazione dell'IA, (2) l'esistenza del legame all'UE richiesto e (3) la categoria di rischio dell'applicazione dell'IA. Dal momento che l'AI

Act è una normativa complessa, è consigliabile consultare esperti legali per valutare queste questioni.

1. In particolare, chiunque sviluppi o faccia sviluppare un sistema di IA e lo immetta sul mercato o lo metta in funzione con il proprio nome o marchio (nell'UE) è considerato un fornitore e quindi soggetto all'AI Act. Se l'applicazione di IA è sviluppata da una terza parte in base alle esigenze e alle istruzioni specifiche della vostra azienda, l'attività di sviluppo sarà probabilmente attribuita alla vostra azienda. D'altro canto, se la vostra azienda "acquista" un sistema di IA esistente o si limita ad adattarne la presentazione al design aziendale, si può sostenere che ciò non costituisca un'attività di sviluppo. Sebbene l'AI Act non prevede il ruolo di fornitore senza l'immissione sul mercato o la messa in servizio nell'UE, questa formulazione contraddice la chiara intenzione del legislatore europeo di assoggettare alla legge sull'IA anche "fornitori e operatori" di Paesi terzi "se l'output prodotto dal sistema di IA viene utilizzato nell'Unione". A causa della differenza tra la formulazione e l'intenzione del legislatore, si dovrebbe ritenere in via precauzionale che le aziende che immettono un sistema di IA sul mercato o lo mettono in funzione al di fuori dell'UE con il proprio nome o marchio siano considerate anch'esse fornitori, purché l'output del sistema di IA sia utilizzato nell'UE.

2. Nel caso in esame, il sistema di intelligenza artificiale è destinato a verificare le domande ricevute in base alla sua finalità, a suggerire le domande idonee e a informare i richiedenti di una decisione positiva o negativa senza ulteriore intervento umano. Si può ipotizzare che la comunicazione della decisione sia andata a buon fine e che l'output del sistema di IA sia "utilizzato" nell'UE e che vi sia un legame sufficiente con l'UE. L'uso dell'output del sistema di IA nell'UE, come descritto sopra, soddisfa i requisiti per il ruolo di fornitore e gli obblighi corrispondenti devono essere osservati.

3. L'entità degli obblighi dell'azienda in qualità di fornitore di sistemi di intelligenza artificiale dipende, in ultima analisi, dalla categoria di rischio in questione. I fornitori di sistemi di IA ad alto rischio sono soggetti agli obblighi più completi. L'AI Act elenca tra le categorie di sistemi di IA ad alto rischio i sistemi che devono essere utilizzati per il reclutamento o la selezione di persone fisiche e che vagliano e filtrano le candidature. Nel caso in questione, è proprio questo il compito previsto del sistema di IA. Di conseguenza, il sistema di IA previsto è un sistema di IA ad alto rischio, il che significa che la vostra azienda deve rispettare requisiti e obblighi completi (ad esempio, gestione del rischio, governance dei dati, documentazione tecnica, supervisione umana, cybersecurity, valutazione della conformità). Anche se c'è ancora tempo per garantire la conformità grazie ai periodi di transizione, è necessario pianificare un tempo sufficiente per l'attuazione delle misure corrispondenti (definizione delle responsabilità e dei processi).

Inoltre, l'elaborazione dei dati rilevanti ai fini del GDPR avviene nell'ambito dell'applicazione AI. Il sistema di IA analizza le domande presentate - e quindi i dati personali - e decide, senza ulteriore intervento umano, se inoltrare la domanda all'utente o inviare una decisione negativa al richiedente. Nel caso di trattamenti di dati che comportano decisioni individuali automatizzate, potrebbe essere necessario osservare requisiti speciali (ad esempio, informazioni sul diritto a un'"audizione umana" e sul diritto di presentare osservazioni). Ulteriori obblighi rimangono riservati.

11. Esempio di caso III: Chatbot

Sono responsabile dell'acquisto e dell'introduzione di un chatbot sul nostro sito web. Il chatbot fornirà agli utenti svizzeri e stranieri informazioni sui nostri prodotti e servizi e risponderà a semplici domande su di essi. Cosa devo considerare dal punto di vista normativo?
L'implementazione del chatbot sul sito web, che si rivolge (anche) a utenti di altri Paesi dell'UE, porterà in questo caso probabilmente all'applicazione dell'AI Act (si veda l'esempio di caso II per i requisiti).

Un chatbot non è di per sé un sistema di intelligenza artificiale ad alto rischio, motivo per cui i relativi fornitori e operatori non sono soggetti a requisiti e obblighi completi. Ma devono soddisfare alcuni requisiti, in particolare per quanto riguarda la trasparenza. L'AI Act stabilisce che le persone devono essere informate del fatto che stanno interagendo con un sistema di IA, a meno che ciò non sia ovvio a causa delle circostanze. Tuttavia, questo obbligo si applica solo ai fornitori, non all'operatore. Se la vostra azienda sviluppa o fa sviluppare il chatbot, dovete fornire informazioni adeguate nell'ambito del processo di progettazione e sviluppo. Se, invece, acquistate il chatbot come "soluzione standard" da una terza parte, la vostra azienda potrebbe, a determinate condizioni, qualificarsi solo come operatore del sistema di IA e quindi non essere soggetta all'obbligo di trasparenza.

Non è (ancora) definitivamente chiaro quando esista esattamente un'attività di sviluppo e quindi lo status di provider ai sensi dell'AI Act. Tuttavia, la questione della misura in cui il "chatbot standard" di un provider può essere personalizzato in base alle esigenze individuali di un'azienda senza che l'azienda stessa diventi un provider a seguito di tali personalizzazioni è probabilmente di notevole importanza pratica. Esistono numerosi modi per adattare un sistema di IA alle esigenze individuali di un'azienda (ad esempio specificando "prompt", addestrandosi su dati specializzati [il cosiddetto "fine-tuning"] o utilizzando modelli basati su query [la cosiddetta "retrieval augmented generation"]). Il fattore decisivo è probabilmente il fatto che il sistema di IA in quanto tale venga (ulteriormente) sviluppato come risultato degli aggiustamenti. Questo potrebbe essere il caso del fine-tuning, perché in questo caso si interferisce con il modello su cui si basa il sistema. Per il RAG, invece, si potrebbe fare un ragionamento diverso, perché non è il sistema di IA in sé a essere personalizzato, ma solo i dati a cui si può accedere come parte dell'applicazione di IA.

Prima dell'acquisto e dell'introduzione del chatbot, è necessario chiarire la questione dello status di fornitore e dell'adempimento degli obblighi corrispondenti, se necessario insieme al fornitore. Il chatbot non dovrebbe essere adattato dopo la sua implementazione senza una preventiva consultazione con il servizio legale, poiché tali adattamenti possono portare a un cambiamento del ruolo dell'azienda (da operatore a fornitore) e quindi a obblighi aggiuntivi. Per fare chiarezza sulle applicazioni di IA utilizzate in azienda e sul rispettivo ruolo dell'azienda, è consigliabile tenere un elenco. Oltre al caso d'uso e al ruolo o agli obblighi previsti dalla legge sull'IA, questo può contenere anche informazioni sul rispettivo proprietario del sistema, sui contratti con terzi, sul trattamento dei dati e sulla valutazione dei rischi.

Infine, è utile emanare direttive e/o istruzioni d'uso sull'uso dei sistemi di IA o dei chatbot per garantire la conformità e sensibilizzare i collaboratori.