HIMMEL ADVISORS

ENIA

Artificial Intelligence

L'utilizzo di sistemi di AI nel contesto lavorativo. I primi concetti

Novembre 2024

Per qualsiasi necessità si prega, gentilmente, di visitare il nostro sito web
www.himmeladvisors.it/artificialintelligence

1. Obiettivi del Regolamento (UE) 1689/2024

Il Regolamento (UE) 1689/2024 sull'intelligenza artificiale (AI Act), proposto dalla Commissione Europea nel 2021, mira a stabilire un **quadro giuridico di riferimento** per l'uso di sistemi di AI all'interno dell'UE

In particolare stabilisce regole armonizzate volte a disciplinare la **produzione**, la **distribuzione** e l'**impiego dell'intelligenza artificiale** nel mercato interno. Inoltre, questo regolamento si propone di garantire che l'IA sia sicura, rispettosa dei diritti fondamentali e delle normative europee e nazionali di settore (in particolare il GDPR e la Direttiva NIS2)

Pur non essendo il Regolamento concepito per disciplinare l'impiego delle tecnologie intelligenti nell'ambito lavorativo, esso istituisce **obblighi di conformità dettagliati a carico dei datori di lavoro e genera significative ripercussioni sulle dinamiche delle relazioni industriali**

Terminologia specifica del Regolamento

2. Terminologia

Sistema di AI: sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali

Esempio

Un esempio comune di sistema di AI è Siri, l'assistente virtuale di Apple. Siri è in grado di riconoscere i comandi vocali e di rispondere a domande in modo naturale, permettendo agli utenti di interagire facilmente. Grazie all'apprendimento automatico, migliora nel tempo adattandosi alle preferenze individuali. Inoltre, Siri può integrarsi con diverse funzioni del dispositivo, come inviare messaggi, controllare il meteo e riprodurre musica. Siri è considerato un sistema di AI, tra gli altri, perché utilizza il riconoscimento vocale per comprendere i comandi degli utenti, trasformando la voce in testo e analizzando il significato delle richieste.

2. Terminologia

Deployer (c.d. utilizzatore): una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale

Esempio

INAF
ISTITUTO NAZIONALE DI ASTROFISICA

Immaginiamo che l'Istituto Nazionale di Astrofisica (INAF) utilizzi un sistema di intelligenza artificiale per analizzare i dati provenienti da telescopi spaziali, al fine di scoprire nuovi pianeti e analizzare le caratteristiche delle stelle. In questo scenario, qualora vi fossero i presupposti di legittimità, l'INAF potrebbe sviluppare un algoritmo di AI che esamina enormi quantità di immagini e dati spettroscopici raccolti dai telescopi, identificando automaticamente schemi e anomalie che potrebbero indicare la presenza di nuovi esopianeti o eventi astrofisici. L'INAF potrebbe quindi utilizzare l'AI, come deployer, per condurre ricerche scientifiche avanzate nel campo dell'astrofisica.

2. Terminologia

Deployer (c.d. utilizzatore): una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale

Attenzione

Se il *deployer* è una persona fisica che utilizza sistemi di IA nel corso di un'attività «non professionale» e «puramente personale» il regolamento (UE) 1689/2024 non è applicabile

2. Terminologia

Distributore: una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione

Esempio

Microsoft offre soluzioni di intelligenza artificiale attraverso la sua piattaforma cloud Azure. Microsoft funge da distributore di sistemi di intelligenza artificiale alle aziende e organizzazioni dell'UE. Le organizzazioni possono utilizzare i servizi di AI offerti da Azure, come strumenti di machine learning e analisi dei dati, per sviluppare applicazioni personalizzate e soluzioni innovative. In questo caso, Microsoft distribuisce un sistema di intelligenza artificiale sul mercato, consentendo alle organizzazioni di sfruttare le potenzialità della tecnologia senza dover sviluppare internamente tali competenze.

2. Terminologia

Finalità prevista: l'uso di un sistema di IA previsto dal fornitore, compresi il contesto e le condizioni d'uso specifici, come dettagliati nelle informazioni comunicate dal fornitore nelle istruzioni per l'uso, nel materiale promozionale o di vendita e nelle dichiarazioni, nonché nella documentazione tecnica

Attenzione

Mai confondere le «finalità previste» relative a un sistema di intelligenza artificiale con le «finalità del trattamento» secondo il GDPR.

Le prime si riferiscono agli obiettivi specifici per cui il sistema è progettato e le modalità di utilizzo indicate dal fornitore. Queste finalità descrivono il contesto e le condizioni d'uso del sistema. Le "finalità del trattamento dei dati", invece, riguardano gli scopi per cui i dati personali vengono raccolti e utilizzati all'interno di un trattamento. In sostanza, le finalità previste si concentrano sull'uso del sistema nel suo complesso, mentre le finalità del trattamento dei dati riguardano la gestione delle informazioni.

2. Terminologia

Dati di addestramento: i dati utilizzati per addestrare un sistema di IA adattandone i parametri che può apprendere

Esempio

Un insieme di testi utilizzati per addestrare un sistema di intelligenza artificiale di elaborazione del linguaggio naturale (NLP). In questo caso, i dati di addestramento potrebbero consistere in un vasto corpus di articoli, libri, conversazioni e post sui social media, comprensivi di diverse lingue e stili di scrittura. Ogni pezzo di testo potrebbe essere etichettato con informazioni utili, come le emozioni espresse (positivo, negativo, neutro) o il tema principale. Durante il processo di addestramento, il modello analizza questi testi per apprendere le regole grammaticali, le relazioni semantiche e le strutture linguistiche. In questo modo, il sistema diventa capace di generare testi coerenti, comprendere il contesto delle frasi e persino rispondere a domande in modo pertinente.

2. Terminologia

Verifica biometrica: la verifica automatizzata e uno a uno, inclusa l'autenticazione, dell'identità di persone fisiche mediante il confronto dei loro dati biometrici con i dati biometrici forniti in precedenza

Esempio

Sistema di riconoscimento delle impronte digitali utilizzato negli smartphone. Quando un utente imposta il proprio telefono, può registrare le proprie impronte digitali. Durante il processo di sblocco del dispositivo, il sistema di riconoscimento delle impronte digitali confronta l'impronta digitale scansionata con quelle salvate nel database del telefono. Se corrispondono, il telefono si sblocca e consente l'accesso al dispositivo. Questo tipo di verifica biometrica sfrutta caratteristiche uniche delle impronte digitali per confermare l'identità dell'utente, garantendo così un livello di sicurezza elevato.

2. Terminologia

Sistema di categorizzazione biometrica: la verifica automatizzata e uno a uno, inclusa l'autenticazione, dell'identità di persone fisiche mediante il confronto dei loro dati biometrici con i dati biometrici forniti in precedenza

Esempio

Un software di analisi delle emozioni che utilizza dati biometrici, come le espressioni facciali o la scansione del volto, per classificare le persone in diverse categorie emotive, come felice, triste, arrabbiato o neutro. In questo scenario, l'IA analizza le immagini del volto di una persona tramite telecamere o foto per rilevare le espressioni e i parametri biometrici, come la posizione e l'angolo delle sopracciglia o la curvatura delle labbra. Basandosi su questi dati, il sistema può assegnare una categoria emotiva alla persona in tempo reale. Questo tipo di categorizzazione biometrica può essere utilizzato in applicazioni come il marketing, dove le aziende vogliono capire come i consumatori reagiscono a un prodotto o a una pubblicità.

A chi si applica il Regolamento (UE) 1689/2024 sull'AI?

3. Ambito di applicazione del Regolamento (UE) 1689/2024 (art. 2)

- **fornitori** che immettono sul mercato o mettono in servizio sistemi di IA, indipendentemente dal fatto che siano stabiliti/ubicati nell'UE o un paese terzo
- **deployer** dei sistemi di IA che hanno il loro luogo di stabilimento o sono situati all'interno dell'Unione
- **fornitori e deployer** di sistemi di IA che hanno il loro luogo di stabilimento o sono situati in un paese terzo, laddove l'**output prodotto dal sistema di IA sia utilizzato nell'Unione**
- **Importatori, distributori e fabbricanti** di sistemi di IA
- **rappresentanti autorizzati di fornitori**, non stabiliti nell'Unione
- **persone interessate** che si trovano nell'Unione
- **sistemi di IA classificati come ad alto rischio**

3. Ambito di applicazione del Regolamento (UE) 1689/2024: sistemi esclusi

Software "automatici" programmati per eseguire un compito sulla base della logica di automazione statica e deterministica della sequenza *if-than*

Esempio «Sistema di gestione delle mail»

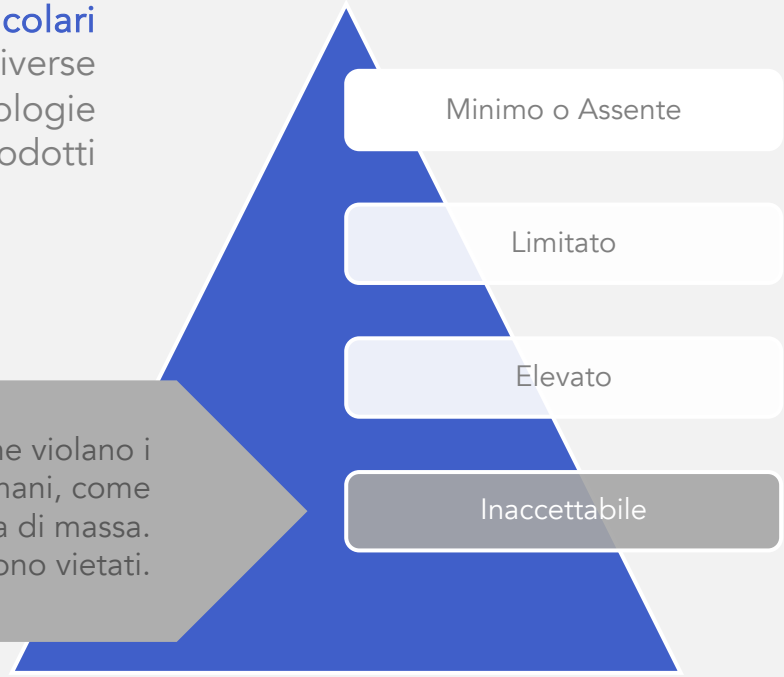
Immagina un sistema di posta elettronica che utilizza filtri per organizzare automaticamente le email in arrivo. In questo caso, il software esegue un'azione specifica ogni volta che la condizione è soddisfatta. Non ci sono variazioni o adattamenti nel processo, poiché il comportamento del software è predeterminato e segue rigidamente la logica "if-then". Ogni volta che arriva un'email da quel mittente, il sistema applicherà automaticamente la stessa regola senza considerare ulteriori contesti o fattori esterni.

Il Regolamento (UE) 1689/2024 non si applica a tali sistemi

Classificazione del rischio associato ai sistemi di AI

4. Risk-based approach

Il legislatore europeo ha definito il **grado di rischio associato a particolari impieghi dell'AI** e definito **regimi di responsabilità differenziati** per le diverse soggettività coinvolte nella catena di approvvigionamento delle tecnologie intelligenti (fornitori, utilizzatori, importatori, distributori, fabbricanti di prodotti che incorporano AI, rappresentanti autorizzati, terzi).

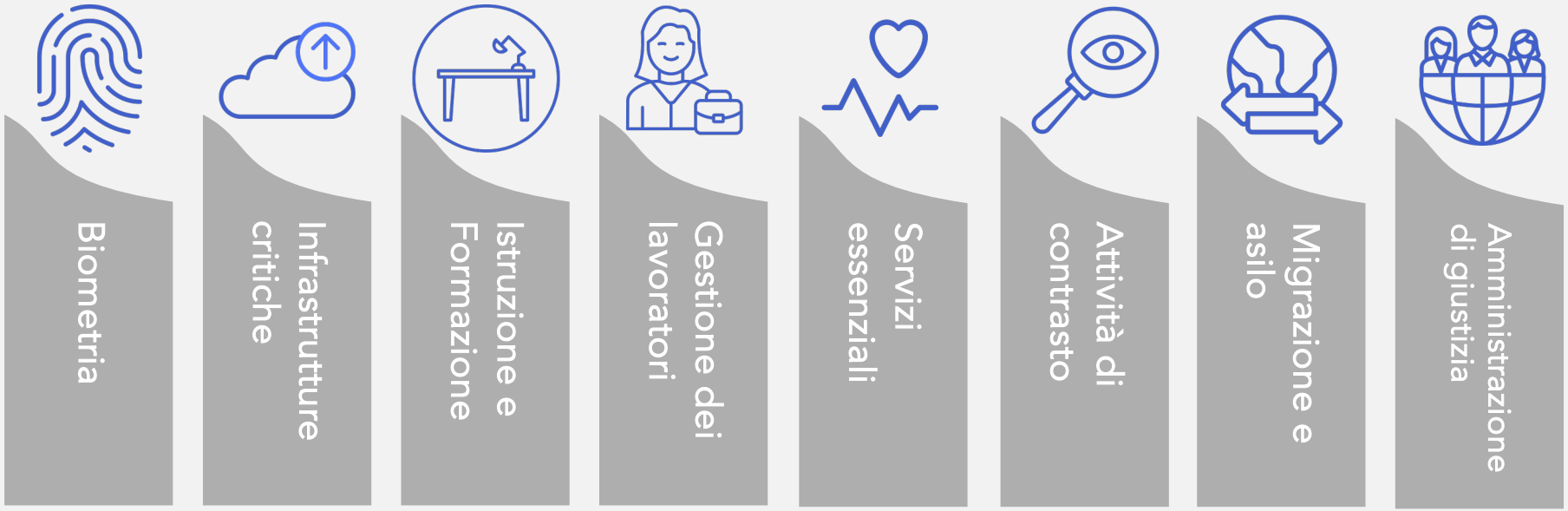


I sistemi di social score in questo contesto possono sollevare preoccupazioni relative alla privacy, alla trasparenza e all'equità. Le decisioni basate su punteggi potrebbero non sempre riflettere accuratamente la capacità di una persona di ripagare un prestito, specialmente se i dati utilizzati non sono completi o accurati.

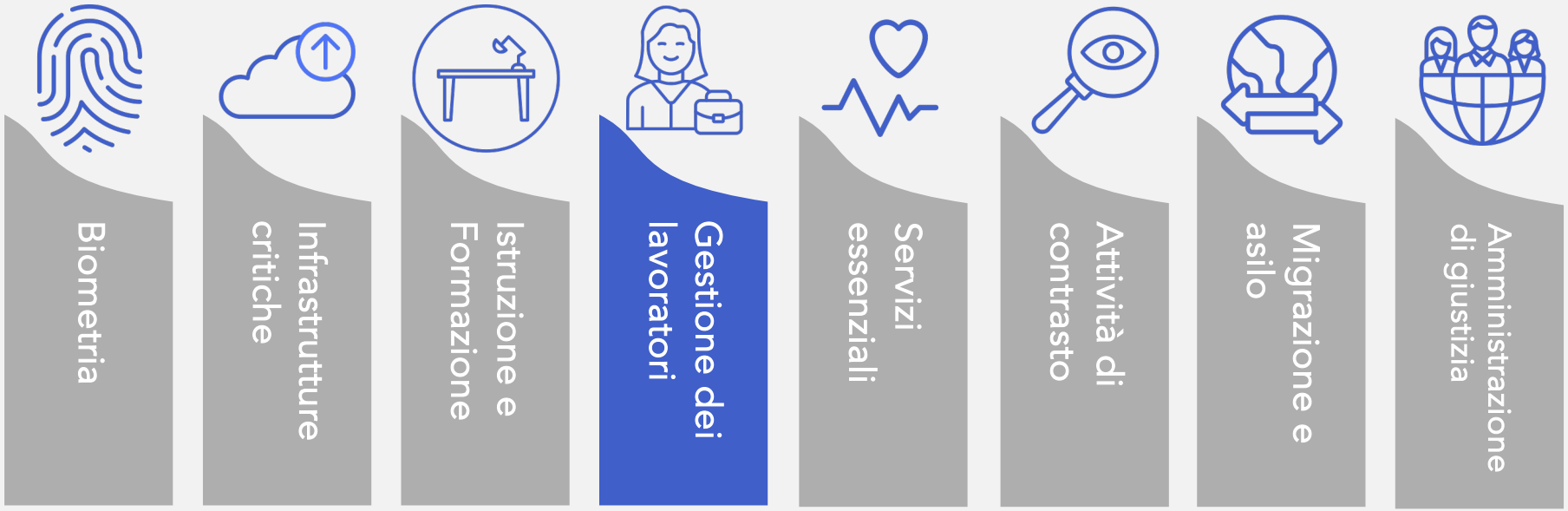
Questa categoria comprende sistemi che violano i valori fondamentali dell'UE o i diritti umani, come il punteggio sociale o la sorveglianza di massa. Tali sistemi sono vietati.

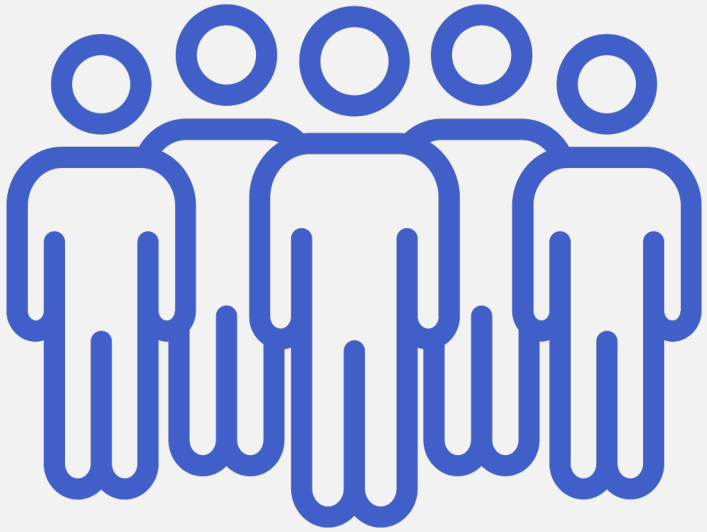
Quali sono i sistemi di AI ad alto rischio?

5. Sistemi di AI ad alto rischio: categorizzati in settori



5. Sistemi di AI ad alto rischio: categorizzati in settori





Artificial Intelligence nel contesto lavorativo

6. AI sul posto di lavoro

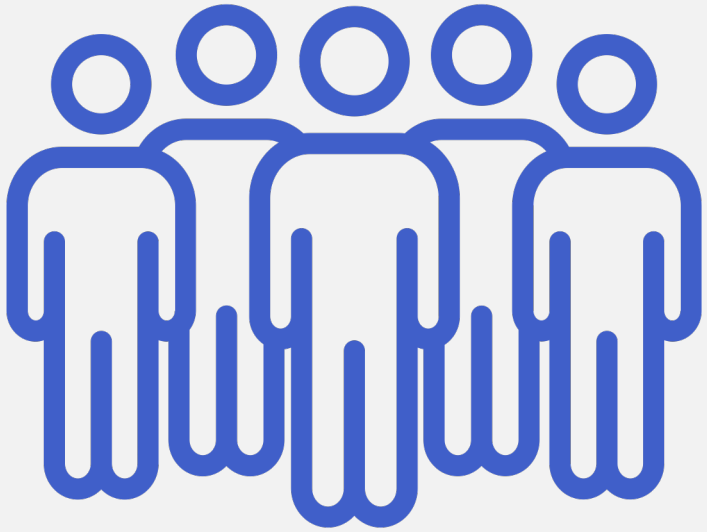
L'Allegato III del Regolamento (UE) 2024/1689 identifica le applicazioni settoriali dell'IA a cui si associa un grado di "rischio elevato", in particolare nel **settore dell'occupazione, della gestione dei lavoratori e dell'accesso al lavoro autonomo**

CANDIDATI

- Assunzione e selezione del personale
- Pubblicazione di annunci di lavoro mirati
- Analisi e filtraggio delle candidature
- Valutazione dei candidati e delle candidate

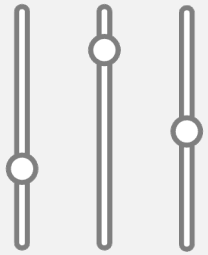
PERSONALE

- Adozione di decisioni riguardo le condizioni lavorative
- Promozione o cessazione dei rapporti contrattuali di lavoro
- Assegnazione di compiti sulla base del comportamento
- Monitoraggio e valutazione delle prestazioni del lavoratore



Artificial Intelligence sul posto di lavoro e datori di lavoro (*deployer*)

7. Obblighi in capo ai datori di lavoro o *deployer* (utilizzatori di sistemi di AI)



Governance

assicurare che l'impiego dell'IA avvenga secondo le impostazioni e le finalità stabilite dal fornitore

Si suggerisce di provvedere ad effettuare controlli e audit regolari, insieme al proprio IT e DPO, al fine di verificare che il sistema utilizzato viene impiegato correttamente

Transparency & Information

evitare che il ricorso all'IA possa essere occultato ai destinatari

Si consiglia di informare, ai sensi dell'art. 13 e 14 GDPR i soggetti sottoposti a processi in cui viene utilizzato un sistema di AI

Risk-Enhancement

rafforzare la strategia di gestione dei rischi, permettendo l'identificazione di quei pericoli che non sono evincibili nelle fasi di progettazione e sviluppo

Si propone di organizzare riunioni regolari con un gruppo multidisciplinare ed esperti di sicurezza nonche altri utilizzatori. Queste riunioni potrebbero servire a discutere nuovi rischi emergenti e scenari non considerati a priori

7. Obblighi in capo ai datori di lavoro o *deployer* (utilizzatori di sistemi di AI)

Sistemi vietati

è vietato l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito lavorativo (candidati, collaboratori e personale in generale)

Se un responsabile volesse utilizzare un sistema IA per analizzare le espressioni facciali o le tonalità della voce dei membri del team per determinare le loro emozioni in tempo reale, ciò sarebbe vietato

Definizione delle pratiche

Il datore di lavoro adotta pratiche di gestione dei dati adeguate alla finalità prevista dal sistema al fine di assicurarne la pertinenza, la rappresentatività, la correttezza e completezza dei dati trattati, l'appropriatezza in relazione alla popolazione di riferimento ed in relazione all'ambito geografico in cui opera il sistema di AI.

Fundamental Rights Impact Assessments (FRIA)

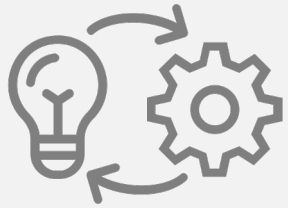
è obbligatoria per i datori di lavoro che utilizzano sistemi di intelligenza artificiale, poiché consente di identificare e mitigare i rischi per i diritti e le libertà dei dipendenti oppure bloccare il trattamento in fase «by design»

La FRIA dovrebbe essere effettuata dal Titolare del trattamento e (si suggerisce) venga condotta dal DPO che dovrà dimostrare di avere competenze in materia

7. Obblighi in capo ai datori di lavoro o *deployer* (utilizzatori di sistemi di AI)

Formazione del personale

i membri del team deputato alla gestione del sistema di AI dovrebbero essere formati sulle normative di protezione dei dati e sulle best practices per gestire gli strumenti di IA, al fine di minimizzare i rischi e rispettare i diritti dei dipendenti



Procedimentalizzazione

È fondamentale procedimentalizzare e formalizzare l'utilizzo dell'AI nel contesto lavorativo. Questo implica l'adozione di procedure chiare che regolamentano l'implementazione e l'uso dei sistemi di IA, assicurando così la trasparenza, la responsabilità e la conformità alle normative vigenti

ISO 27001*

L'integrazione con la certificazione ISO 27001 costituisce un primo step dimostrare l'adeguamento dei propri sistemi a standard internazionali più elevati

Si pensi all'adozione di misure di controllo adeguate e procedure di gestione dei rischi che siano in linea con i requisiti della certificazione, contribuendo così a proteggere i dati sensibili e a garantire la conformità alle normative di protezione dei dati.

**La ISO 27001 non è un vero obbligo in capo al datore di lavoro in quanto è uno strumento di soft law*

8. Implementazione di Technical and Organizational Security Measures (TOSM-AI)

- alfabetizzazione del datore di lavoro nonché dei soggetti deputati alla gestione e l'utilizzo del sistema di AI. L'art. 4 del Regolamento (UE) 1689/2024 impone agli utilizzatori (ma anche ai fornitori di sistemi AI) di adottare misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati

- sorveglianza umana quale misura di sicurezza che ogni datore di lavoro che utilizza un sistema di AI deve implementare nei propri processi. In particolare, la sorveglianza umana mira a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, in particolare qualora tali rischi persistano. Le misure di sorveglianza sono commisurate ai rischi, al livello di autonomia e al contesto di utilizzo del sistema di IA ad alto rischio e sono garantite mediante almeno «misure individuate e integrate nel sistema di AI» e »misure individuate dal fornitore prima dell'immissione sul mercato o messa in servizio e adattate ad essere attuate dall'utilizzatore»

- accuratezza, robustezza e cibersicurezza quali principi applicabili ai sistemi di AI ad alto rischio, in fase di sviluppo e durante tutto il ciclo di vita al fine di operare materialmente e dal punto di vista della sicurezza delle informazioni in modo coerente nonché trasparente. Tali principi devono essere anche rispettati dai deployer o utilizzatori (datori di lavoro)

8. Implementazione di Technical and Organizational Security Measures (TOSM-AI)

- resilienza del sistema di AI rispetto a errori, malfunzionamenti o incongruenze. I sistemi di IA ad alto rischio sono il più resilienti possibile per quanto riguarda errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente in cui esso opera, in particolare a causa della loro interazione con persone fisiche o altri sistemi

- robustezza dei sistemi che può essere conseguita mediante soluzioni tecniche di ridondanza, che possono includere piani di backup o fail-safe. Il datore di lavoro, insieme ai propri tecnici, dovrebbe verificare che il sistema di AI che intende utilizzare è stato sviluppato in modo tale da eliminare o ridurre il più possibile il rischio di output potenzialmente distorti che influenzano gli input per operazioni future (feedback loops - «circuiti di feedback») e cercare di garantire, durante tutto il periodo di utilizzo dei sistemi, che tali circuiti di feedback siano oggetto di adeguate misure di attenuazione

- misure per governare le vulnerabilità dei sistemi di AI utilizzati dai datori di lavoro. In particolare, il datore di lavoro, insieme ai propri tecnici, è tenuto a verificare che i sistemi di IA ad alto rischio sono resilienti ai tentativi di terzi non autorizzati di modificarne l'uso, gli output o le prestazioni sfruttando le vulnerabilità del sistema. Le soluzioni tecniche da implementare dovrebbero essere adeguate alle circostanze e ai rischi pertinenti. Le soluzioni tecniche finalizzate ad affrontare le vulnerabilità specifiche dell'IA dovrebbero includere, ove opportuno, da parte del datore di lavoro, misure volte a prevenire, accertare, rispondere, risolvere e controllare gli attacchi che cercano di manipolare il set di dati di addestramento (data poisoning - «avvelenamento dei dati») o i componenti preaddestrati utilizzati nell'addestramento (model poisoning - «avvelenamento dei modelli»), gli input progettati in modo da far sì che il modello di IA commetta un errore (adversarial examples - «esempi antagonistici», o model evasion, - «evasione dal modello»), gli attacchi alla riservatezza o i difetti del modello

8. Implementazione di Technical and Organizational Security Measures (TOSM-AI)

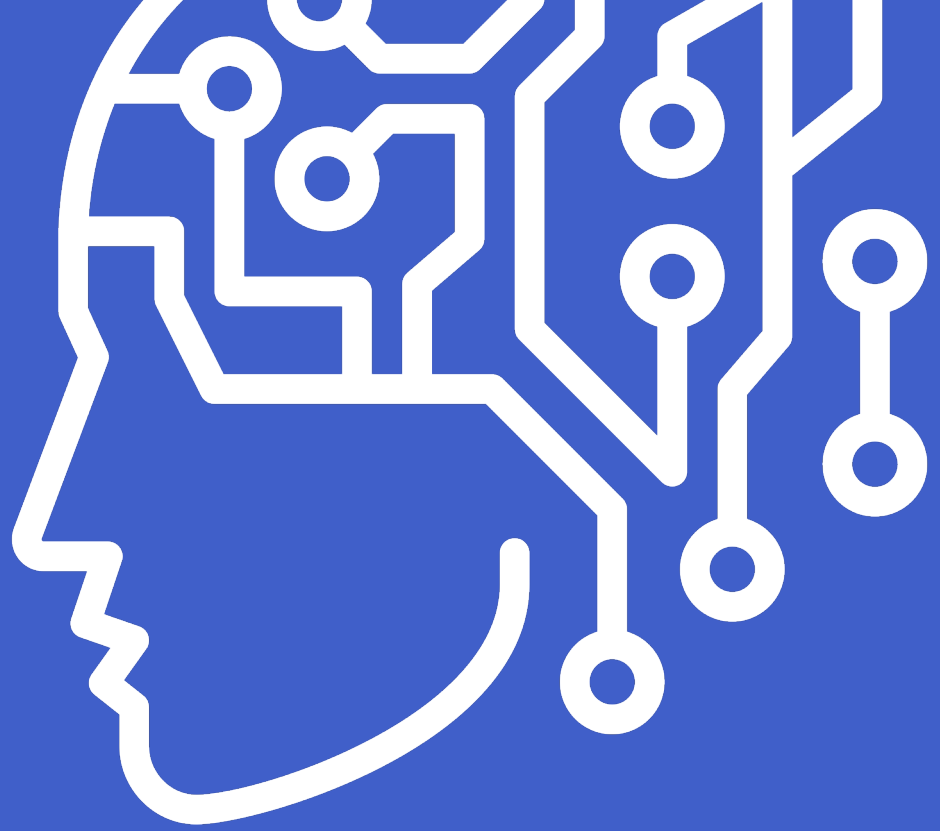
- monitoraggio e mitigazione dei rischi riguardo il funzionamento del sistema di IA ad alto rischio sulla base delle istruzioni per l'uso. I datori di lavoro ed i propri tecnici sono tenuti ad informare i fornitori a tale riguardo. Qualora abbiano motivo di ritenere che l'uso del sistema di IA ad alto rischio in conformità delle istruzioni possa comportare che il sistema di IA presenti un rischio, i datori di lavoro ne informano, senza indebito ritardo, il fornitore o il distributore e la pertinente autorità di vigilanza del mercato e sospendono l'uso di tale sistema. Qualora abbiano individuato un incidente grave, i datori di lavoro ne informano immediatamente anche il fornitore, in primo luogo, e successivamente l'importatore o il distributore e le pertinenti autorità di vigilanza del mercato. Nel caso in cui il datore di lavoro non sia in grado di raggiungere il fornitore, si applica mutatis mutandis l'articolo 73 del Regolamento (UE) 1689/2024

- conservazione dei log generati automaticamente tramite i sistemi di AI utilizzati dai datori di lavoro. In particolare, i datori di lavoro devono conservare i log generati automaticamente dal sistema utilizzato, nella misura in cui tali log sono sotto il loro controllo (o del proprio IT), per un periodo adeguato alla prevista finalità del sistema di IA ad alto rischio, di almeno sei mesi

L'importanza di un coordinamento interno tra i diversi esperti in materia, tra cui i collaboratori responsabili dell'utilizzo dei sistemi di AI e i consulenti esterni, è fondamentale per garantire la compliance normativa e la protezione dei dati personali. Tale coordinamento deve includere la consultazione del consulente privacy e, ove nominato, del DPO, al fine di effettuare una valutazione adeguata delle misure di sicurezza tecniche e organizzative adottate nell'ambito dei sistemi di IA. Questo approccio collaborativo è essenziale per garantire il rispetto del GDPR e della Direttiva NIS2. Un'accurata valutazione delle misure di sicurezza non solo contribuisce a prevenire incidenti di sicurezza, ma è altresì cruciale per evitare potenziali sanzioni derivanti dalla mancata valutazione dei sistemi utilizzati o da un uso inadeguato degli stessi.

HIMMEL ADVISORS

ENIA



Artificial Intelligence

L'utilizzo di sistemi di AI nel contesto lavorativo
I primi concetti

Novembre 2024

Dr. Francisco Garcia
Legal Counsel & Privacy Officer
E. garcia@himmeladvisors.it

www.himmeladvisors.it/**artificialintelligence**