

Dove passano i confini: divieti, decisioni sulle persone e trasparenza

Conta l'uso, non solo lo strumento. Nel dubbio: fermarsi, chiedere, segnalare.

CONCETTI CHIAVE

Conta l'uso, non solo lo strumento

Lo stesso assistente è a rischio minimo per la documentazione tecnica e può diventare ad alto rischio se usato per selezionare candidature. La domanda giusta: per che cosa lo si usa, e chi riguarda?

Pratiche vietate (dal 2 febbraio 2025)

Riconoscimento delle emozioni da dati biometrici sul luogo di lavoro (salvo motivi medici o di sicurezza delle persone); categorizzazione biometrica per dedurre razza, opinioni politiche e altre caratteristiche sensibili; manipolazione e sfruttamento delle vulnerabilità che causano, o possono causare, danni significativi; punteggio sociale. Sanzioni fino a 35 milioni di euro o al 7% del fatturato mondiale annuo, se superiore (per le PMI, l'importo minore).

Alto rischio: selezionare, valutare, monitorare

Selezione e colloqui, promozioni e cessazioni, assegnazione dei compiti, monitoraggio, merito creditizio (Allegato III dell'AI Act). Non vietati: obblighi dell'AI Act dal 2 dicembre 2027, ma già oggi valgono GDPR, informativa al personale e regole sul controllo a distanza. Non si avviano per iniziativa personale; chi lavora in proprio ne verifica prima gli obblighi.

L'ultima parola a una persona

Art. 22 GDPR: diritto a non subire decisioni basate solo su un trattamento automatizzato con effetti significativi, salvo eccezioni previste e con garanzie. Revisione umana reale. Il datore di lavoro informa chi lavora e le rappresentanze sindacali sui sistemi decisionali o di monitoraggio integralmente automatizzati (d.lgs. 152/1997, art. 1-bis).

Trasparenza (art. 50)

Il fornitore progetta: avviso nei chatbot che dialogano con le persone, anche interni; marcatura dei contenuti generati. Il deployer (l'organizzazione che usa lo strumento, o chi lavora in proprio) dichiara i deep fake e i testi pubblicati su questioni di interesse pubblico, salvo revisione umana con responsabilità editoriale. Per l'AI Act, i testi per uso interno non richiedono dichiarazioni.

Deep fake e persone reali

Al lavoro, per prudenza: volto e voce di una persona reale solo con il suo consenso. Dal 2 dicembre 2026 è vietato usare l'IA per generare contenuti intimi realistici di persone riconoscibili senza consenso o materiale di abuso sessuale su minori, e immettere sul mercato sistemi pensati per farlo. Diffondere senza consenso contenuti falsificati con l'IA e credibili, causando un danno ingiusto, è reato (art. 612-quater c.p.: reclusione da 1 a 5 anni).

L'IA dentro i programmi

Attivare una funzione nuova equivale a usare uno strumento nuovo. Trascrizioni e verbali automatici delle riunioni: solo se previsti, informando prima chi partecipa. Misurare l'umore dal volto o dalla voce sul lavoro è vietato.

Nuovi usi e segnalazioni

Prima di un nuovo uso: chiedere, classificare, registrare; cinque segnali per fermarsi. Errori e anomalie si segnalano subito: se una violazione di dati personali va notificata, l'organizzazione (o chi lavora in proprio) la comunica all'autorità di norma entro 72 ore da quando ne viene a conoscenza.

IL CORSO IN DIECI REGOLE

1. Conta l'uso, non solo lo strumento.
2. Plausibile non significa vero: verificare fatti, fonti e norme.
3. Usare solo strumenti autorizzati, con l'account di lavoro; in proprio, piani professionali.
4. Un dato inviato non si ritira: mai credenziali; dati personali e informazioni riservate solo se è espressamente previsto.
5. L'assistente propone, una persona decide.
6. Le pratiche vietate non si usano mai, nemmeno per prova.
7. Selezionare, valutare o monitorare persone con l'IA: mai per iniziativa personale; in proprio, verificarne prima gli obblighi.
8. Le decisioni rilevanti sulle persone spettano a una persona.
9. Si dichiarano i deep fake e, se non rivisti, i testi di interesse pubblico.
10. Nel dubbio: fermarsi, chiedere, segnalare.