CORSO IA CON CLAUDE · DISPENSA PER L'ALLIEVO

Normativa, privacy, ecologia ed etica

Le regole europee, i dati aziendali, l'impronta ambientale e i limiti dell'IA

ORA	DURATA	MODULO
02 di 12	60 minuti	1 — Quadro giuridico

Gianluca Bonomo · www.gianlu.it · info@gianlu.it

Indice

Indice 2
Come usare questa dispensa 3
1. Perché servono delle regole 4
2. L'AI Act europeo 4
2.1 Quattro livelli di rischio 5
2.2 Il calendario di applicazione 6
2.3 Che cosa cambia in pratica per chi usa un chatbot 7
2.4 L'Italia: la legge 132/2025 7
3. Privacy: i dati che escono dalla porta 8
3.1 Il GDPR in cinque principi 9
3.2 Il rischio si chiama data leakage 10
3.3 Shadow AI: il nemico invisibile 10
3.4 Due casi italiani da conoscere 11
3.5 Account personale o abbonamento aziendale? 11
4. L'impronta ambientale 12
4.1 Energia 12
4.2 Acqua 13
4.3 Il paradosso di Jevons 14
4.4 Green AI: che cosa possiamo fare noi 14
5. Etica: bias e allucinazioni 15
6. Esercitazione: audit di risk assessment 17
Glossario 18
Per approfondire 20

Come usare questa dispensa

Questa dispensa raccoglie, in forma scritta e ordinata, tutto quello che vediamo insieme durante l'ora di lezione. Non devi studiarla a memoria: serve a farti ritrovare le cose con calma, dopo, quando l'aula è finita e ti resta una domanda in sospeso.

È pensata per chi parte da zero. Ogni termine tecnico viene spiegato la prima volta che compare, e a fine dispensa trovi un glossario con tutte le parole nuove. Se una pagina ti sembra difficile, saltala e torna indietro dopo: nessun concetto di questa dispensa richiede conoscenze informatiche precedenti.

> **COME SONO FATTI I RIQUADRI**
>
> **In parole semplici** (azzurro): la spiegazione senza tecnicismi, quella da portarsi a casa se si ricorda una cosa sola.
>
> **Attenzione** (oro): un errore frequente, un rischio, una cosa da non fare.
>
> **Esempio** (grigio): un caso concreto, preso dalla vita di tutti i giorni o dal lavoro in azienda.

Obiettivo dell'ora

Avere il quadro completo di ciò che sta intorno allo strumento: la regolamentazione europea (AI Act), la protezione dei dati aziendali (GDPR), l'impatto ambientale dell'IA e i dilemmi etici legati a bias e allucinazioni. Sono gli argomenti che in aula si saltano quasi sempre, e che invece decidono se l'IA in azienda è un vantaggio o un problema.

Che cosa saprai fare alla fine

- Riconoscere a quale livello di rischio dell'AI Act appartiene uno strumento che già usi.
- Sapere che cosa non va mai incollato dentro un chatbot, e perché.
- Distinguere un account personale gratuito da un abbonamento aziendale idoneo.
- Farti un'idea concreta del costo energetico e idrico di ogni richiesta.
- Compilare una prima scheda di valutazione del rischio per la tua azienda.

1. Perché servono delle regole

Le regole sull'IA non sono materia per giuristi. Definiscono che cosa si può fare, chi risponde se qualcosa va storto e quali diritti abbiamo come cittadini e come lavoratori.

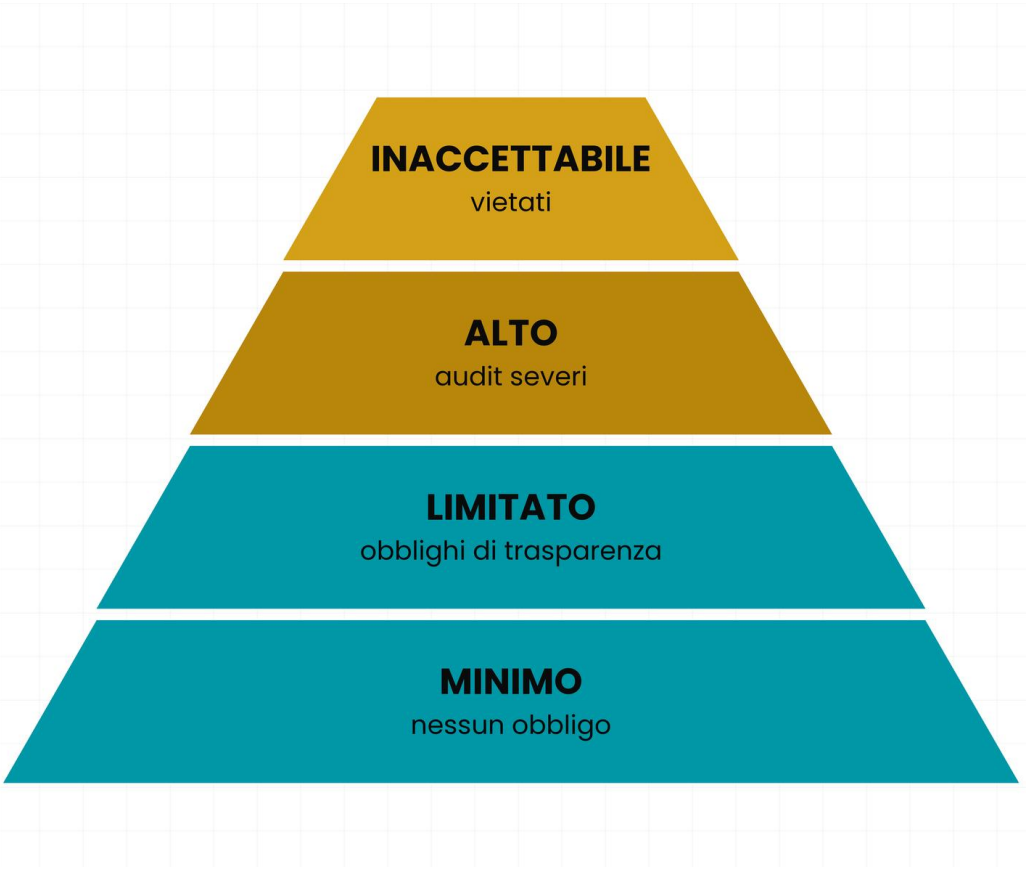
Il problema di fondo è quello che abbiamo visto nell'ora precedente: spesso non è possibile ricostruire *perché* un sistema di IA ha preso una certa decisione. Diventa quindi difficile capire se qualcuno è stato trattato ingiustamente — in una selezione del personale, in una richiesta di mutuo, in un accesso a un servizio pubblico. Le leggi esistenti offrono qualche tutela, ma non bastano.

> **IL PRINCIPIO DI FONDO**
>
> L'Europa non regola *la tecnologia*: regola **l'uso che se ne fa**. Lo stesso modello linguistico può essere innocuo se scrive una newsletter e ad alto rischio se seleziona curriculum. Quello che conta è il contesto.

2. L'AI Act europeo

Il Regolamento (UE) 2024/1689, universalmente noto come **AI Act**, è il primo quadro giuridico organico sull'intelligenza artificiale al mondo. Pubblicato in Gazzetta Ufficiale europea il 12 luglio 2024, è entrato in vigore il 1° agosto 2024 e si applica per gradi.

2.1 Quattro livelli di rischio



L'approccio dell'AI Act: più alto è il rischio per le persone, più stringenti sono gli obblighi.

Livello	Che cosa comprende	Che cosa comporta
Rischio inaccettabile	Nove pratiche vietate: manipolazione dannosa, sfruttamento di vulnerabilità, punteggio sociale, previsione del rischio criminale individuale, raccolta indiscriminata di volti dal web, riconoscimento delle emozioni sul lavoro e a scuola, categorizzazione biometrica di caratteristiche protette, identificazione biometrica remota in tempo reale, generazione di contenuti intimi non consensuali e materiale pedopornografico.	**Vietati.** I primi otto divieti si applicano dal 2 febbraio 2025; il nono, introdotto in un secondo momento, dal 2 dicembre 2026.
Rischio alto	Infrastrutture critiche, istruzione, componenti di sicurezza dei prodotti, selezione del personale e gestione dei lavoratori, accesso a servizi essenziali come il credito, identificazione biometrica, forze dell'ordine, migrazione e	Obblighi severi: valutazione e mitigazione del rischio, qualità dei dati, tracciabilità, documentazione tecnica, informazione all'utilizzatore, **supervisione umana**, robustezza e cybersicurezza.

Livello	Che cosa comprende	Che cosa comporta
	frontiere, giustizia e processi democratici.	
Rischio di trasparenza	Chatbot, assistenti virtuali e in generale i sistemi che generano testi, immagini, audio e video.	L'utente deve sapere che sta interagendo con una macchina; i contenuti generati devono essere identificabili, e i *deepfake* e i testi di informazione pubblica vanno etichettati in modo chiaro e visibile.
Rischio minimo o nullo	La stragrande maggioranza dei sistemi in uso: filtri antispam, videogiochi, sistemi di raccomandazione.	Nessun obbligo specifico dall'AI Act.

DOVE RICADE IL CHATBOT CHE USI OGNI GIORNO

Un assistente come ChatGPT o Claude, usato per scrivere e riassumere, ricade nel **rischio di trasparenza**: pochi obblighi, tutti orientati a far capire alle persone che stanno parlando con una macchina.

Ma lo **stesso** strumento, usato per filtrare curriculum o per valutare la solvibilità di un cliente, diventa un sistema **ad alto rischio**, con obblighi molto più pesanti. Non cambia la tecnologia: cambia l'uso.

2.2 Il calendario di applicazione

L'AI Act non è entrato in vigore tutto insieme. Il calendario è scaglionato per dare alle imprese il tempo di adeguarsi, ed è già stato modificato una volta: il pacchetto di semplificazione noto come *Omnibus* ha spostato in avanti gli obblighi per i sistemi ad alto rischio.

Data	Che cosa scatta
1° agosto 2024	Entrata in vigore del regolamento. Nessun obbligo ancora applicabile.
2 febbraio 2025	Divieti sulle pratiche inaccettabili (i primi otto) e obbligo di **alfabetizzazione all'IA**: chi impiega sistemi di IA deve garantire che il personale che li usa abbia un livello adeguato di conoscenze.
2 agosto 2025	Regole per i modelli per finalità generali (GPAI), governance, riservatezza e prime disposizioni sanzionatorie.
2 agosto 2026	Si applica **il resto del regolamento**, compresi gli obblighi di trasparenza dell'articolo 50. È il passaggio che tocca più da vicino chi usa chatbot in azienda.

Data	Che cosa scatta
2 dicembre 2026	Entra in vigore il nono divieto (contenuti intimi non consensuali e materiale pedopornografico generati da IA). Chi aveva già sul mercato sistemi che generano contenuti sintetici deve essersi adeguato all'articolo 50(2).
2 agosto 2027	I modelli GPAI immessi sul mercato prima del 2 agosto 2025 devono essere conformi.
2 dicembre 2027	Scattano gli obblighi per i sistemi **ad alto rischio** dell'Allegato III (lavoro, credito, istruzione, giustizia…). Erano originariamente previsti per agosto 2026.
2 agosto 2028	Obblighi per i sistemi ad alto rischio che sono componenti di prodotti regolati (Allegato I).

Calendario verificato a settembre 2026 su digital-strategy.ec.europa.eu e artificialintelligenceact.eu.

2.3 Che cosa cambia in pratica per chi usa un chatbot

Dal **2 agosto 2026** si applicano gli obblighi di trasparenza. In concreto:

- Chi mette a disposizione un chatbot deve far capire alle persone che stanno **interagendo con un sistema di IA**, non con un collega.
- I contenuti generati artificialmente devono essere **identificabili**: testi, immagini, audio, video.
- I **deepfake** e i testi pubblicati per informare il pubblico su questioni di interesse pubblico vanno **etichettati in modo chiaro e visibile**.

> **TRADOTTO PER LA TUA AZIENDA**
>
> Se pubblichi sul sito una risposta automatica alle domande dei clienti, deve essere evidente che risponde un assistente virtuale.
>
> Se usi l'IA per generare l'immagine di una campagna o il testo di un comunicato destinato al pubblico, quella natura artificiale va dichiarata.
>
> Non è un adempimento astratto: è esattamente il punto in cui l'AI Act tocca il lavoro quotidiano di chi fa comunicazione e assistenza clienti.

Le sanzioni non sono simboliche: per le violazioni più gravi l'AI Act prevede multe fino al **7% del fatturato annuo globale** dell'impresa.

2.4 L'Italia: la legge 132/2025

L'Italia è stata il primo Stato membro dell'Unione a dotarsi di una normativa nazionale organica complementare all'AI Act: la **legge 23 settembre 2025, n. 132**, in vigore dal **10**

ottobre 2025. Non sostituisce il regolamento europeo: lo integra con principi nazionali e deleghe al Governo.

Le autorità nazionali designate sono l'**Agenzia per l'Italia digitale (AgID)** e l'**Agenzia per la cybersicurezza nazionale (ACN)**.

I punti che riguardano il lavoro

- **Obbligo di informazione**: il datore di lavoro deve informare i lavoratori — e le rappresentanze sindacali — dell'uso di sistemi di IA.
- **Divieto di discriminazione algoritmica**: le decisioni automatizzate non possono generare discriminazioni per genere, età, origine etnica, credo religioso o condizione sociale.
- **Supervisione umana**: le decisioni sui rapporti di lavoro non possono essere completamente automatizzate, e il lavoratore ha diritto a conoscere criteri e logica delle decisioni che lo riguardano.
- **Professioni intellettuali**: l'uso dell'IA deve restare strumentale e di supporto, senza mai sostituire il lavoro intellettuale del professionista.
- **Osservatorio nazionale** presso il Ministero del Lavoro, per monitorare i settori più esposti e sostenere la formazione continua.

Sul fronte penale, la legge inasprisce le pene per i reati commessi mediante sistemi di IA, inclusa la diffusione illecita di *deepfake*.

3. Privacy: i dati che escono dalla porta

È il punto in cui l'entusiasmo per lo strumento può diventare un problema legale per l'azienda. E quasi sempre non c'entrano gli hacker: c'entra un copia-e-incolla fatto in buona fede.

3.1 Il paradosso dell'IA

Per funzionare bene, l'IA ha bisogno di dati. Tantissimi. Più è utile, più dati personali rischia di assorbire; più ne assorbe, più diventa potente; e più diventa potente, più è difficile controllare che cosa sa di noi.



L'obiettivo è semplice da enunciare e difficile da praticare: i dati aziendali devono restare dentro il perimetro.

3.1 Il GDPR in cinque principi

In Europa la protezione dei dati personali è regolata dal **GDPR**, in vigore dal 2018. Non è stato scritto per l'IA, ma si applica eccome. I principi da ricordare:

- **Liceità, correttezza e trasparenza**: le persone devono sapere che cosa succede ai loro dati.
- **Limitazione della finalità**: i dati si raccolgono per uno scopo preciso e dichiarato, non "per ogni evenienza".
- **Minimizzazione**: si raccoglie solo quello che serve davvero.
- **Limitazione della conservazione**: non si tengono più a lungo del necessario.
- **Integrità e riservatezza**: vanno protetti.

L'IA mette sotto pressione proprio questi principi. Come si garantisce la limitazione della finalità, se un modello viene addestrato su dati raccolti per uno scopo e poi usato per mille scopi diversi? E come si concilia la minimizzazione con modelli affamati di quantità sempre maggiori di dati?

L'AI Act **non sostituisce** il GDPR: lo integra, aggiungendo obblighi specifici su trasparenza, documentazione, supervisione umana e gestione del rischio.

3.2 Il rischio si chiama data leakage

Immagina la scena. Marco ha una scadenza urgente e un foglio di calcolo pieno di nomi di clienti, fatturati e margini. Apre un chatbot gratuito, carica il file e scrive: «analizza questi dati e scrivimi un riassunto». In trenta secondi ha il suo report. Ha fatto bella figura.

Quello che Marco non ha considerato è che quei dati ora sono su un server che la sua azienda non controlla, gestito da un fornitore con cui l'azienda non ha alcun contratto. Sono usciti dal perimetro. E non tornano indietro.

> **SU CHI RICADE LA RESPONSABILITÀ**
>
> In caso di violazione, le sanzioni del GDPR ricadono **sull'azienda**, non sul dipendente che ha agito in autonomia. È il motivo per cui questo tema non riguarda solo l'ufficio IT.

Che cosa non va mai incollato in un chatbot pubblico

- Dati anagrafici e di contatto di clienti, fornitori, dipendenti.
- Contratti, listini, margini, informazioni commerciali riservate.
- Codice sorgente e documentazione tecnica proprietaria.
- Dati sanitari, giudiziari, e in generale le **categorie particolari** del GDPR.
- Password, credenziali, chiavi di accesso, codici fiscali, coordinate bancarie.

3.3 Shadow AI: il nemico invisibile

Il fenomeno di Marco ha un nome: **Shadow AI**, IA ombra. Indica l'uso spontaneo e non autorizzato di strumenti di IA esterni da parte dei dipendenti, all'insaputa dell'IT e della direzione. Non serve una tecnica di attacco sofisticata: basta un copia-e-incolla.

Il danno non è solo la fuga di dati. È che la Shadow AI rende **invisibile il flusso delle informazioni**: l'azienda non sa quali dati siano usciti, non può controllarne l'uso e non può dimostrare di aver fatto il necessario per proteggerli.

> **COME SI AFFRONTA DAVVERO**
>
> Non con i divieti assoluti, che spingono le persone a nascondersi meglio. Con tre mosse:
>
> **1. Fornire un'alternativa ufficiale.** Se il dipendente usa un chatbot pubblico, spesso è perché l'azienda non gliene dà uno autorizzato.
>
> **2. Formare.** Le persone devono sapere con precisione che cosa possono condividere e che cosa no, e perché.
>
> **3. Costruire una cultura della trasparenza.** Se dichiarare di usare l'IA non espone a

rimproveri, il fenomeno emerge e si può governare.

3.4 Due casi italiani da conoscere

OpenAI e il Garante Privacy

Il Garante per la protezione dei dati personali ha sanzionato **OpenAI** con **15 milioni di euro** (provvedimento del 2 novembre 2024, reso noto a dicembre), contestando carenze di trasparenza verso gli utenti, una raccolta non proporzionata di dati per l'addestramento, l'assenza di verifica dell'età e l'omessa comunicazione di una violazione dei dati. Alla sanzione si accompagnava l'obbligo di una campagna informativa di sei mesi.

AGGIORNAMENTO: LA SANZIONE È STATA ANNULLATA

Il **20 marzo 2026** il Tribunale di Roma ha **annullato** la sanzione. La decisione si fonda su una questione di competenza — quale autorità europea fosse titolata a istruire un caso transfrontaliero (il meccanismo dello *sportello unico* del GDPR) — e **non entra nel merito** delle contestazioni sulla privacy.

È una distinzione che vale la pena capire: il fatto che una sanzione cada per un vizio di competenza non significa che i problemi sostanziali non esistessero.

DeepSeek

Il 30 gennaio 2025, pochi giorni dopo il lancio globale del chatbot cinese **DeepSeek**, il Garante ha adottato d'urgenza un provvedimento di limitazione del trattamento dei dati degli utenti italiani, contestando la raccolta di dati tramite *web scraping* senza basi legali sufficienti, l'assenza di un'informativa in lingua italiana e la violazione degli obblighi di trasparenza. L'app è stata rimossa dagli store italiani.

3.5 Account personale o abbonamento aziendale?

	Account consumer gratuito	Abbonamento aziendale
Dati di input	Possono essere usati per addestrare i modelli futuri, salvo disattivare l'opzione (dove esiste, e non sempre è facile trovarla).	Esclusi dall'addestramento per contratto.
Contratto	Nessun accordo sul trattamento dei dati fra azienda e fornitore.	Condizioni contrattuali e responsabilità definite.

	Account consumer gratuito	Abbonamento aziendale
Governo	Uso “in ombra”, fuori da ogni policy aziendale.	Accessi, ruoli e amministrazione centralizzata.
Tracciabilità	Nessuna: non si sa chi ha condiviso cosa.	Registro degli accessi e delle attività.
In caso di controllo	L'azienda non può dimostrare di aver adottato misure adeguate.	L'adozione è dichiarata e verificabile.

> **PRIMA DI RINUNCIARE ALL'IA**
>
> Nessuno di questi rischi è un buon motivo per non usare l'intelligenza artificiale, così come i virus non sono un buon motivo per rinunciare a internet. Sono un buon motivo per usarla con gli strumenti giusti.

4. L'impronta ambientale

È il tema del capitolo 9 del libro, e quello che in aula sorprende di più: ogni richiesta che scriviamo ha un costo fisico, fatto di elettricità e di acqua.

4.1 Energia

Per quasi vent'anni il consumo elettrico dei data center era rimasto sorprendentemente stabile, nonostante il traffico internet crescesse di venti volte: l'efficienza compensava la crescita. Poi, fra la fine del 2022 e l'inizio del 2023, la curva si è impennata.

Indicatore	Valore	Fonte
Consumo elettrico globale dei data center, 2024	circa **415 TWh**, pari a circa l'**1,5%** del consumo elettrico mondiale	IEA, *Energy and AI*
Proiezione al 2030	circa **945 TWh**, poco meno del **3%** del consumo mondiale: un raddoppio	IEA, *Energy and AI*
Crescita dei data center dedicati all'IA nel 2025	**+50%** in un anno, a fronte di una domanda elettrica globale cresciuta del 3%	IEA
Investimenti delle cinque maggiori aziende tecnologiche, 2025	oltre **400 miliardi di dollari**, con previsione di crescita del 75% nel 2026	IEA

Addestramento e inferenza: due cose diverse

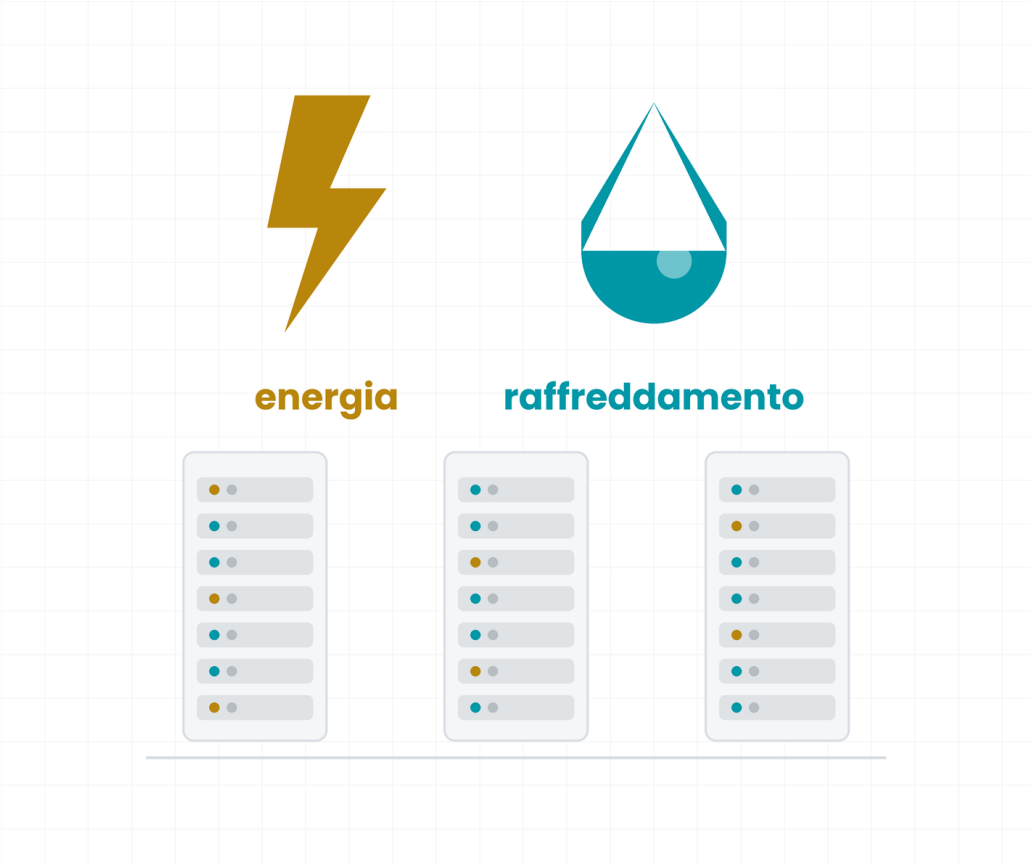
Il ciclo di vita di un modello ha due fasi con costi molto diversi.

- L'**addestramento** è la fase in cui il modello impara: intensiva, concentrata nel tempo, con migliaia di schede grafiche che lavorano ventiquattr'ore al giorno per settimane. È come mandare un ragazzo a scuola per dodici anni: costoso, ma si fa una volta.
- L'**inferenza** è la fase in cui il modello, già addestrato, risponde alle nostre domande. Il costo della singola risposta è minuscolo, ma moltiplicato per miliardi di interazioni al giorno diventa il peso maggiore.

Fino al 2022 l'addestramento era la voce dominante. Oggi non più: è l'inferenza — cioè l'uso quotidiano che ne facciamo noi — ad aver preso il sopravvento.

4.2 Acqua

L'energia è solo metà della storia. I data center consumano anche acqua dolce, spesso potabile, per il **raffreddamento evaporativo** dei server. E le schede grafiche che eseguono i calcoli dell'IA scaldano molto più dei processori tradizionali.



Due risorse, un solo conto: elettricità per far funzionare i server, acqua per raffreddarli.

C'è poi un consumo idrico che non si vede: quello necessario a **produrre l'elettricità** che alimenta i data center. Secondo le analisi di settore è la parte maggiore del totale, e cresce insieme al consumo energetico.

> **PERCHÉ I NUMERI SULL'ACQUA VANNO PRESI CON LE PINZE**
>
> Non esiste uno standard condiviso per misurare e dichiarare il consumo idrico di una richiesta. Le stime pubblicate variano di due ordini di grandezza: Google ha dichiarato circa **0,26 millilitri** per una richiesta testuale mediana a Gemini, Mistral circa **45 millilitri** per una risposta di 400 token, e altre analisi indipendenti collocano le richieste testuali fra 10 e 50 millilitri.
>
> La differenza dipende dal modello, dal data center, dal clima e da che cosa si decide di contare. **L'assenza di uno standard è essa stessa il problema**: senza dati confrontabili, nessuno può scegliere il fornitore più sostenibile.

4.3 Il paradosso di Jevons

Qui entra in gioco un meccanismo economico osservato nell'Ottocento dall'economista inglese **William Stanley Jevons**: quando una tecnologia diventa più efficiente nell'uso di una risorsa, il consumo *totale* di quella risorsa tende ad aumentare, non a diminuire.

> **LE MACCHINE A VAPORE**
>
> Le macchine a vapore di Watt erano molto più efficienti delle precedenti. Proprio perché erano efficienti ed economiche, furono adottate in tutti i settori industriali. Il consumo totale di carbone esplose.

L'IA sta vivendo esattamente questo. L'efficienza per singola operazione migliora a un ritmo che l'Agenzia Internazionale dell'Energia definisce probabilmente senza precedenti nella storia dell'energia. Ma proprio questa efficienza rende l'IA più economica e accessibile, quindi la usano in più persone, per più cose, con modelli più grandi. Il consumo totale continua a salire.

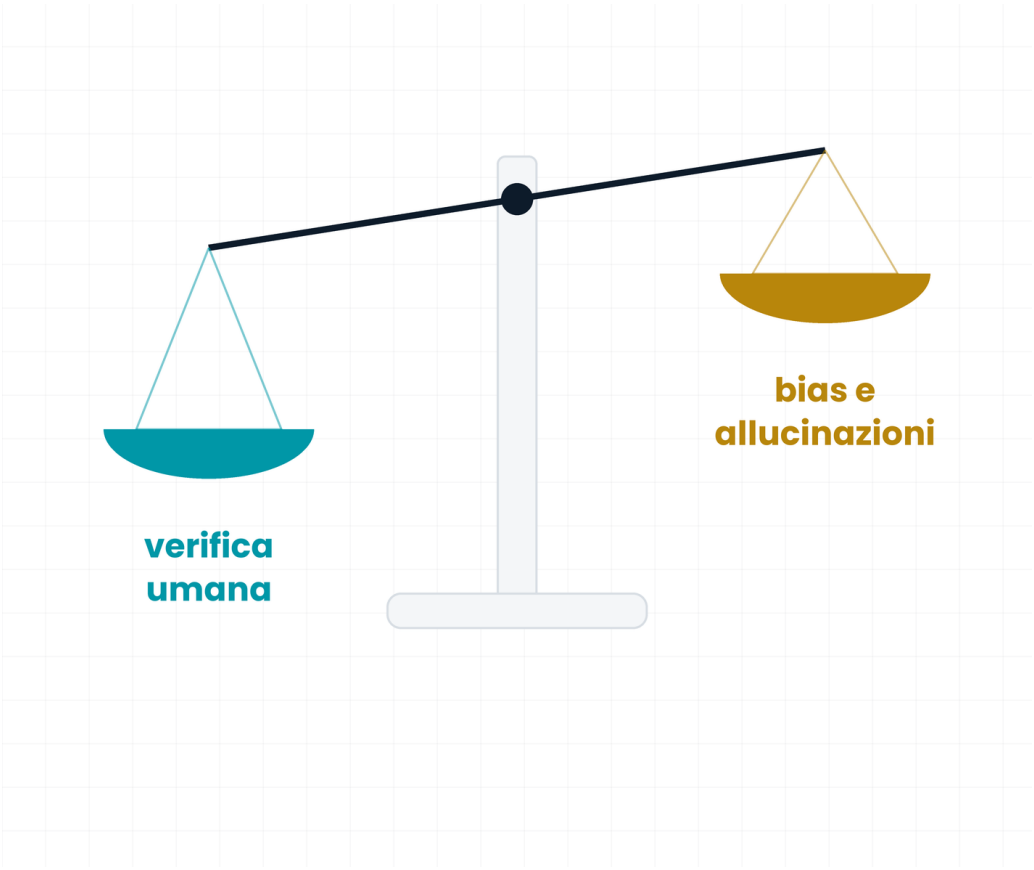
4.4 Green AI: che cosa possiamo fare noi

- **Scegliere il modello adatto al compito.** Non serve sempre il più potente: a un compito semplice basta un modello leggero, che consuma una frazione.
- **Ridurre le richieste inutili.** Ogni query evitata è energia e acqua risparmiate. Le conversazioni lunghe e i tentativi a raffica costano.

- **Scrivere prompt precisi al primo colpo.** Meno tentativi significa meno consumo e, non per caso, anche risposte migliori. Ne parleremo diffusamente con il metodo CO-STAR.
- **Chiedere trasparenza ai fornitori.** Il consumo dichiarato dovrebbe essere un criterio di scelta, come il prezzo.

5. Etica: bias e allucinazioni

Se le allucinazioni sono errori casuali, i bias sono errori sistematici. E sono molto più difficili da scovare.



Il modello produce testo plausibile, non necessariamente vero. La verifica umana è il contrappeso.

5.1 Le allucinazioni

Immagina di chiedere a un amico chi ha scritto *Il Gattopardo*. Risponde con assoluta sicurezza: «Italo Calvino». È sbagliato (è Giuseppe Tomasi di Lampedusa), ma il tono era identico a quello che usa quando ha ragione. E se non conosci la risposta vera, gli credi.

Tecnicamente, un'**allucinazione** è una risposta sintatticamente corretta e plausibile, ma di fatto errata o inventata. Non è un difetto occasionale: è una conseguenza diretta del funzionamento visto nell'ora precedente. Il modello non accede a un archivio di fatti

verificati; genera testo calcolando probabilità. **È un meccanismo di plausibilità, non di verità.**

Per questo le allucinazioni si possono ridurre, contenere, segnalare — ma non eliminare del tutto con l'architettura attuale.

CINQUE DIFESE PRATICHE

Consapevolezza: sapere che il modello può sbagliare con stile convincente è già metà dell'opera.

Verifica incrociata per date, cifre, riferimenti normativi, nomi e citazioni.

Strumenti che citano le fonti: la ricerca web integrata permette di controllare da dove arriva l'informazione.

Segnali d'allarme: risposte troppo dettagliate su argomenti oscuri, fonti che non si trovano altrove, numeri che non tornano.

Mai delegare decisioni con conseguenze serie senza un controllo umano.

5.2 I bias

L'IA viene spesso percepita come un giudice imparziale, proprio perché fatta di numeri e non di emozioni. È una percezione ingannevole. I modelli imparano dai dati, e i dati sono lo specchio della nostra società, con le sue disuguaglianze e i suoi stereotipi.

Il risultato è che l'IA non solo può riprodurre le discriminazioni esistenti, ma può **amplificarle su larga scala**, in modo automatico e spesso invisibile. Le ricerche documentano distorsioni sistematiche nella descrizione dei ruoli professionali per genere ed etnia, e nelle valutazioni automatiche dei curriculum.

Le radici del problema sono tre: i **dati di addestramento**, che riflettono uno specchio deformante della società; la **scatola nera**, cioè l'opacità dei modelli profondi, che rende difficilissimo dimostrare di essere stati discriminati; e la **mancanza di diversità** nei team che sviluppano i sistemi.

LA REGOLA CHE TIENE INSIEME TUTTO

L'IA può assistere, suggerire, velocizzare. Ma la decisione finale, quando tocca i diritti e le opportunità delle persone, **deve restare umana**. Non è solo buon senso: dal 10 ottobre 2025 è anche quello che la legge italiana chiede espressamente nei rapporti di lavoro.

6. Esercitazione: audit di risk assessment

L'esercizio dell'ora. Serve a fotografare la situazione reale della tua azienda, compresi gli strumenti che nessuno ha mai autorizzato.

Primo passo. Elenca i software di IA usati oggi in azienda, inclusi quelli "non ufficiali" che i colleghi usano dal browser o dal telefono personale.

Secondo passo. Per ciascuno, compila la riga della tabella.

Strumento	A cosa serve	Livello di rischio (AI Act)	Account consumer o aziendale?	Che dati ci finiscono dentro
.....	.....	.....	.....	.....
.....	.....	.....	.....	.....
.....	.....	.....	.....	.....
.....	.....	.....	.....	.....

Terzo passo. Per ogni riga in cui compare un account consumer *e* dei dati aziendali, hai trovato un problema da risolvere. Sono quelli da cui partire.

> **IL CRITERIO PER ASSEGNARE IL LIVELLO DI RISCHIO**
>
> Chiediti: **che cosa succede a una persona se il sistema sbaglia?**
>
> Se la risposta è "un testo da riscrivere", sei nel rischio di trasparenza. Se è "un candidato scartato", "un prestito negato" o "una cura sbagliata", sei nell'alto rischio. Se è "nessuna conseguenza", sei nel rischio minimo.

Glossario

Le parole che incontri in questa dispensa, spiegate in una riga. Tienilo a portata di mano: torneranno in tutte le ore successive del corso.

Termine	Che cosa significa
AI Act	Regolamento (UE) 2024/1689, il primo quadro giuridico organico sull'IA al mondo.
Alfabetizzazione all'IA	Obbligo, dal 2 febbraio 2025, di garantire che chi usa sistemi di IA in azienda abbia conoscenze adeguate.
Allucinazione	Risposta plausibile e ben scritta, ma di fatto errata o inventata.
Bias	Distorsione sistematica: un pregiudizio presente nei dati che il modello riproduce e amplifica.
Data leakage	Informazioni riservate che escono dal perimetro aziendale, spesso per un semplice copia-e-incolla.
Deepfake	Contenuto audio, video o fotografico manipolato o generato da IA per far dire o fare a qualcuno cose mai dette o fatte.
GDPR	Regolamento europeo sulla protezione dei dati personali, in vigore dal 2018.
GPAI	*General Purpose AI*: modelli per finalità generali, come i grandi modelli linguistici.
Inferenza	L'uso quotidiano del modello già addestrato. Oggi è la voce energetica più pesante.
Paradosso di Jevons	Quando una tecnologia diventa più efficiente, il consumo totale tende ad aumentare invece che a calare.
Raffreddamento evaporativo	Raffreddamento dei data center che consuma acqua dolce disperdendola in atmosfera.
Shadow AI	Uso di strumenti di IA non autorizzati, all'insaputa dell'IT e della direzione.
Sportello unico	Meccanismo del GDPR che individua un'unica autorità capofila per i casi transfrontalieri.
Supervisione umana	Obbligo di mantenere una persona nel processo decisionale, con potere effettivo di intervenire.
TWh	Terawattora: mille miliardi di wattora. Unità con cui si misura il consumo elettrico su scala nazionale.
Web scraping	Raccolta automatica di dati dal web tramite programmi. Usata per

Termine	Che cosa significa
	costruire i dataset di addestramento.

Per approfondire

Le fonti usate per costruire questa dispensa. Sono tutte pubbliche e consultabili: se un dato ti interessa, vai alla fonte e verificalo. È esattamente quello che chiediamo di fare anche all'intelligenza artificiale.

Il testo dell'AI Act e il quadro ufficiale

Commissione europea, *AI Act* — digital-strategy.ec.europa.eu (pagina aggiornata al 3 agosto 2026). Regolamento (UE) 2024/1689.

Il calendario di applicazione

Implementation Timeline, artificialintelligenceact.eu (aggiornato al 31 agosto 2026), con il riferimento articolo per articolo.

La normativa italiana

Legge 23 settembre 2025, n. 132, *Disposizioni e deleghe al Governo in materia di intelligenza artificiale*, in vigore dal 10 ottobre 2025.

Privacy e provvedimenti del Garante

Garante per la protezione dei dati personali, garanteprivacy.it: provvedimento su OpenAI del 2 novembre 2024 (annullato dal Tribunale di Roma il 20 marzo 2026 per difetto di competenza) e provvedimento d'urgenza su DeepSeek del 30 gennaio 2025.

Energia e data center

International Energy Agency, *Energy and AI* e *Energy demand from AI*, iea.org. È la fonte più autorevole e indipendente su questi numeri.

Uso dell'IA in Europa

Eurostat, statistiche sull'uso dell'intelligenza artificiale da parte degli individui, ec.europa.eu/eurostat.

Il libro di riferimento del corso

Gianluca Bonomo, *Niente paura, è solo IA*, capitoli 8 (sicurezza, privacy e rischi), 9 (impatto ambientale) e 11 (etica e società).

UNA NOTA SULLE DATE

Le norme sull'intelligenza artificiale cambiano in fretta. I dati normativi di questa dispensa sono verificati a **settembre 2026**. Prima di usarli in una decisione aziendale, controlla sempre la fonte ufficiale: il calendario dell'AI Act è già stato modificato una volta.