In diretta

Per le PMI che usano l'IA ogni giorno

AI Act: ultima chiamata prima di agosto 2026

Sei in ritardo, ma **ancora in tempo**. Scopri le mosse giuste da compiere prima della scadenza.

A cura di

Avv. Pierluigi Spera
sphera.legal

Antonio Alaia
namidi.it

Due approcci, un'unica direzione.

LATO GIURIDICO — SPHERA Legal | DATA

Avv. Pierluigi Spera

Founding Partner SPHERA · @avvocatodegliutenti

IN SINTESI

- **DPO certificato** UNI CEI EN 17740:2024
- Esperto esterno **Cattedra 'Informatica Giuridica'** UniMi
- Master e corsi di perfezionamento in **Cybersecurity**, **GDPR** e **AI Act**
- Osservatorio Giustizia Civile **Tribunale Milano**

Esperienza diretta su **aziende tech, startup innovative, fondi di investimento e PA**.

DPO esterno | Audit privacy | Data breach
ISO/IEC 27001 | AI Act compliance | Contenzioso

SEDE: Milano
TELEFONO: 347 372 7403
EMAIL: pierluigi.spera@sphera.legal

LATO DATI & TECNICO — Nami · Data Intelligence

Antonio Alaia

CEO & Co-Founder Nami - Data Intelligence

IN SINTESI

- **Fondata 2023** · Napoli · Milano · Buenos Aires
- **50+ progetti** su 8 settori verticali
- 5 divisioni: **Analytics · Market · AI · Legal · Research**

Approccio *"i grandi player globali alle PMI italiane"* — strategie dati/AI scalate sull'impresa media.

Data Analytics | Market Intelligence | AI Solutions
Supporto dati | Research | Data intelligence

SEDI: Milano · Napoli
TELEFONO: 3939764981
EMAIL: a.alaia@namidi.it

Dalle origini alla regolamentazione: settant'anni verso l'AI Act.

L'ATTO DI NASCITA · 1956

Dartmouth College, Stati Uniti

Workshop estivo in cui nasce la disciplina dell'**Intelligenza Artificiale**.

I PADRI FONDATORI

- **John McCarthy** — conia l'espressione *artificial intelligence*; ideatore del linguaggio LISP
- **Marvin Minsky** — co-fondatore del MIT AI Lab
- **Claude Shannon** — padre della teoria dell'informazione (1948)
- **Nathaniel Rochester** — architetto dell'IBM 701

Da qui due scuole di pensiero: **GOFAI** (IA simbolica) e **connessionismo** (reti neurali) — quest'ultimo modello alla base dell'IA generativa odierna.

70 ANNI DI STORIA

Una traiettoria lunga, non un salto improvviso

2017	Architettura **Transformer** (Google, paper *Attention is All You Need*)
2018	Primo **GPT** (OpenAI)
30 NOV 2022	Rilascio pubblico di **ChatGPT** — cambio di paradigma

Tra Dartmouth e ChatGPT: due **"inverni dell'IA"** (anni '60, '80 – inizio '90), poi la rinascita su **big data, GPU e deep learning**.

Innovazione chiave: il transformer coglie relazioni tra parole anche a distanza notevole nel testo grazie alla *self-attention* (auto-attenzione)

LINEE GUIDA ETICHE UE 2019 · AI HLEG — 7 REQUISITI DELL'IA AFFIDABILE

Sorveglianza umana · robustezza · privacy e data governance · trasparenza · non discriminazione · benessere sociale e ambientale · responsabilità. **L'AI Act li rende vincolanti**

*Il sistema non comprende: imita statistiche. La questione non è l'intelligenza della macchina, ma **l'AI Literacy e la responsabilità umana**.*

— Ziccardi · art. 4 AI Act, obbligo di alfabetizzazione sull'IA

L'approccio europeo: innovazione sì, ma con limiti.

Premessa

L'UE è la **prima al mondo** con una disciplina organica sull'IA: **AI Act (Reg. UE 2024/1689)** — adottato **12 lug 2024**, in vigore **1 ago 2024**, operativo da **ago 2026**, con previsione di estensione ad **ago 2027 (art. 113)** per dare tempo a PMI e start-up.

> ***Non una scelta tecnica, ma giuridica e politica: quali rischi per i diritti accettiamo?***

01 ANTROPOCENTRICO

L'essere umano al centro

- Bilanciare **innovazione** e **diritti fondamentali**.
- L'UE non compete sull'innovazione (dominata da USA/Cina) ma sul **diritto come standard globale** — il *Brussels effect*, già sperimentato col GDPR.
- Principio guida: ***non tutto ciò che è tecnicamente possibile è giuridicamente accettabile*.**
- Centralità di **dignità, non-discriminazione, protezione dati, controllo umano significativo**.

02 RISK-BASED

Regole proporzionate al rischio

- L'intensità degli obblighi è **proporzionata al potenziale danno** a salute, sicurezza, diritti fondamentali.
- Strumenti pro-innovazione: **AI regulatory sandboxes** per testare soluzioni emergenti, sostegno mirato a start-up e PMI.
- Istituzione del **Comitato europeo per l'IA**.

⚠ **AMBITO EXTRATERRITORIALE**

L'AI Act si applica anche a sistemi **sviluppati fuori UE** se l'output è utilizzato nel mercato europeo.

03 TRUST BY DESIGN

La fiducia come asset competitivo

La **trust** non è un vincolo allo sviluppo, ma una **leva competitiva**: solo un'IA affidabile, sicura, trasparente può essere accettata su larga scala.

3 PILASTRI · 7 REQUISITI OPERATIVI

Legalità · Eticità · Robustezza tecnica

Linee guida UE 2019 — AI HLEG

UN TERZO MODELLO

Tra **tecnoliberismo USA** e **imperialismo digitale cinese**.

L'AI Act non frena l'innovazione: la orienta. La domanda europea non è *se* innovare, ma come farlo senza sacrificare la persona.

Che cos'è, giuridicamente, l'IA? E perché il diritto deve regolarla.

01 · LA DEFINIZIONE

L'IA secondo l'AI Act (art. 3)

> *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.*
>
> — Reg. (UE) 2024/1689, art. 3 n. 1

Neutra e adattiva: ML, deep learning, sistemi statistici e logici.

⚠ DATO FONDAMENTALE

Il sistema **non comprende**: imita statisticamente il linguaggio (*token più probabile*).

02 · RESPONSABILITÀ DEL DECIDERE

Dal potere umano al potere algoritmico

- ✓ Una tecnologia diventa **problema giuridico** quando decide sulla vita delle persone.
- ✓ Storicamente a decidere sono stati **esseri umani**: fallibili, ma responsabili.
- ✓ L'IA è **nuova forma di potere decisionale**: non perché "pensa", ma perché incide.
- ✓ La domanda non è *cosa è possibile fare*, ma **cosa è accettabile delegare**.

03 · LA RISPOSTA DELL'AI ACT

Approccio antropocentrico e risk-based

Un anticipo dei 4 livelli di rischio:

- **Inaccettabile** → vietate (**art. 5**): social scoring, biometria real-time
- **Alto** → obblighi rigorosi (**art. 6**) + sorveglianza umana (**art. 14**)
- **Limitato** → trasparenza (**art. 50**)
- **Minimo** → codici di condotta

TUTELA PREVENTIVA · CHIUSURA DEL SISTEMA

FRIA — Fundamental Rights Impact Assessment.

Art. 3 — richiamo e ritiro dei sistemi non conformi.

> *Il diritto nasce per regolare il potere decisionale. La domanda non è cosa la macchina può fare, ma **cosa l'essere umano può delegarle**.*

Le sfide che l'IA pone al giurista.

01 OPACITÀ ALGORITMICA

Black box e dati di addestramento

- Output **non esplicitabili** nemmeno dagli sviluppatori.
- Il modello **non comprende**: correla token su base statistica.
- *Garbage in, garbage out*: bias sistemici (caso **COMPAS,** sistema nordamericano per la concessione della libertà vigilata).

PRINCIPI DI USO EQUO (FAIR USE) · ART. 10 AI ACT

I dataset di addestramento, convalida e prova devono essere **findable, accessible, interoperable, reusable**:

- **Tracciati all'origine** — provenienza, raccolta e finalità documentate (specie per dati personali).
- **Preparati correttamente** — etichettatura, pulizia e aggregazione coerenti.
- **Rappresentativi** — pertinenti, completi e statisticamente adeguati ai destinatari del sistema.

02 GDPR + AI ACT

Perchè non basta il GDPR

Dall'art. 22 GDPR all'art. 14 AI Act: dal divieto alla regola operativa.

Il GDPR protegge il dato · risponde a: come trattiamo le informazioni personali? (base giuridica, informativa, DPIA, retention)

L'AI Act protegge la persona dal sistema · risponde a: quel sistema può essere usato? con quali garanzie? chi lo controlla? (artt. 5, 6, 14, 50)

Insieme proteggono la decisione automatizzata · art. 22 GDPR (no decisioni unicamente automatizzate) trova nell'art. 14 AI Act la sua traduzione per i sistemi alto rischio

03 FILIERA

La catena della responsabilità

Accountability su **tutta la filiera**:

- **Provider** — sviluppa e immette sul mercato
- **Deployer** — utilizza professionalmente il sistema
- **Supervisore umano** — **controllo significativo (art. 14)**
- **Importatori & distributori** — obblighi proporzionati

Il **nodo centrale** di questa catena: senza **AI Literacy** (art. 4) le norme restano sulla carta.

⚠ SANZIONI AI ACT

fino a 35 M€

o **7% del fatturato globale**

Opacità · Rischio · Responsabilità — tre nodi che lato legale si devono saper sciogliere a monte, non a valle.

L'art. 14 in dettaglio: la sorveglianza umana.

Per i sistemi alto rischio **non basta che ci sia:** l'umano deve poter esercitare un controllo effettivo.

01 COMPRENSIONE

Conoscere capacità e limiti

Chi supervisiona deve conoscere **logiche, contesti d'uso e divieti**.

→ Serve **formazione specifica** (art. 4).

02 ⚠ IL RISCHIO PIÙ SOTTILE

Distorsione dell'automazione

Fidarsi acriticamente perché *"lo ha detto la macchina"*.

→ Mantenere **giudizio autonomo**, anche se il sistema sembra affidabile.

03 KILL SWITCH

Intervento e arresto

Possibilità — tecnica e organizzativa — di **sospendere, correggere o disattivare**.

→ Non un'opzione: **un requisito**.

⚠ ANTI-PATTERN DA EVITARE

- ✕ **"Approva tutto in 2 click"** — non è supervisione, è ratifica.
- ✕ **Assenza di autorità reale** di intervenire o arrestare → responsabilità delegate in astratto ma non in concreto.
- ✕ **Assenza di formazione adeguata** → responsabilità trasferita ma non gestita.

COLLEGAMENTO GDPR

Art. 22 GDPR → Art. 14 AI Act

Il diritto a non essere soggetti a decisioni **unicamente automatizzate** — qui la sua **traduzione operativa** per l'alto rischio.

L'AI Act: rischi · responsabilità · trasparenza.

Ad ogni tipologia di rischio → corrispondono obblighi differenziati lungo la filiera

➤ PROVIDER · ARTT. 16 ss. chi sviluppa e immette sul mercato

Gestione del rischio · qualità dei dati · documentazione tecnica · **valutazione di conformità ex ante** · registrazione nella banca dati UE · sorveglianza post-commercializzazione · notifica incidenti gravi.

➤ DEPLOYER · ARTT. 26 ss. ← TU chi utilizza professionalmente

Uso conforme alle istruzioni · **sorveglianza umana significativa** (art. 14) · monitoraggio del funzionamento · conservazione dei log · cooperazione con le autorità.

RISCHIO MINIMO

Nessun obbligo specifico

Solo **codici di condotta volontari** (es. Asseprim – Codice di condotta sull'utilizzo dell'IA per le imprese dei servizi professionali).

ESEMPI

Filtri antispam · ottimizzazione logistica · traduzione automatica · videogiochi · sistemi di raccomandazione di film o musica.

RISCHIO LIMITATO · ART. 50

Obblighi di trasparenza

L'utente deve sapere di **interagire con una macchina**. I contenuti sintetici (deepfake, audio, immagini, video generati) devono essere **segnalati come tali**.

ESEMPI

Chatbot · assistenti virtuali · sistemi generativi di contenuti.

ALTO RISCHIO · ART. 6

Conformità ex ante

Gestione rischio · qualità dataset · doc · **tracciabilità log** · informativa · robustezza · cybersicurezza.

ART. 14 · SORVEGLIANZA UMANA

L'umano deve poter: **(a)** comprendere limiti, **(b)** evitare distorsione automazione, **(c)** intervenire/arrestare (kill switch).

ESEMPI

Sanità · istruzione · occupazione · giustizia · servizi essenziali · credito · infrastrutture · frontiere · dispositivi medici, veicoli.

INACCETTABILE · ART. 5

Divieto assoluto

Pratiche **incompatibili con i valori europei**.

ESEMPI

Social scoring (PA) · manipolazione subliminale · sfruttamento vulnerabilità (minori, anziani, disabilità) · biometria real-time in spazi pubblici · categorizzazione biometrica su dati sensibili · riconoscimento emozioni a scuola/lavoro · scraping facciale.

> *La piramide del rischio è **il cuore operativo** dell'AI Act: traduce il principio antropocentrico in **regole concrete e proporzionate**, distribuite lungo l'intera catena del valore — dal provider al deployer.*

Il punto in cui siamo.

Sull'AI Act si dice dappertutto che *"tanto è tutto rimandato"*. È una mezza verità che sta facendo accumulare alle aziende italiane un **debito di conformità pericoloso**.

1 AGO 2024

Entrata in vigore

Il Reg. (UE) 2024/1689 entra in vigore con applicazione progressiva.

FEB 2025 · ATTIVO

Divieti + AI literacy

Art. 5 (pratiche vietate) e **art. 4** (alfabetizzazione) pienamente operativi.

AGO 2025 · ATTIVO

GPAI + sanzioni

Obblighi sui modelli generali (trasparenza, documentazione tecnica, politiche sul diritto d'autore) e **art. 99** sanzionatorio operativi.

→ SEI QUI · GIU 26

Digital Omnibus

Approvata la risoluzione del 16 giugno 2026 che ricalibra le scadenze.

Cosa significa per la tua azienda

Alfabetizzazione, divieti, trasparenza GPAI e sanzioni sono **pienamente esigibili oggi**. Il tempo guadagnato dal rinvio Omnibus non è tempo per attendere — è tempo per organizzarsi.

+ Italia: Legge 132/2025 già in vigore — obblighi specifici per i professionisti

Cos'è l'Omnibus Digitale sull'IA e cosa cambia.

✓ Stato dell'arte · accordo raggiunto

Il Parlamento ha approvato il testo il **16 giugno 2026** a seguito dell'accordo di trilogo del **7 maggio 2026**. Il rinvio sui sistemi ad alto rischio è ora **confermato e definitivo**.

Un pacchetto modificativo dell'AI Act

L'Omnibus semplifica l'attuazione dell'AI Act e di alter normative, a fronte di **ritardi tecnici** nella preparazione delle norme armonizzate e nella designazione delle autorità nazionali.

I 4 obiettivi principali

01 **Evitare il blocco del mercato** — collegare le norme alto rischio agli standard tecnici disponibili, con date ultime certe per la prevedibilità.

02 **Ridurre oneri amministrativi** — estendere i privilegi PMI alle medie imprese (fino a 499 dipendenti).

03 **Contrastare nuovi rischi** — divieti immediati su contenuti sessuali intimi senza consenso (rischio emerso dopo il testo originale).

04 **Armonizzare la vigilanza** — centralizzare il controllo dei sistemi più complessi presso l'Ufficio europeo per l'IA.

⚠ Dal 16 GIU 2026

Il Nuovo Assetto dell'Omnibus Digitale

Accordo Definitivo

Il Parlamento ha ratificato la risoluzione P10_TA(2026)0198 che ricalibra il calendario per i sistemi ad alto rischio, fissando le scadenze al **2 dicembre 2027** per i sistemi stand-alone (Allegato III) e al **2 agosto 2028** per i sistemi integrati in prodotti regolamentati (Allegato I). Restano pienamente esigibili i divieti e gli obblighi GPAI già scattati tra il 2024 e il 2025

Semplificazione

Le **misure di favore per le PMI e le start-up** (come la documentazione tecnica semplificata e la gestione della qualità agevolata) sono ufficialmente estese anche alle piccole imprese a media capitalizzazione (small mid-caps). Viene inoltre garantito loro un **accesso prioritario e gratuito agli spazi di sperimentazione normativa** (sandbox) e una particolare attenzione alla **sostenibilità economica nel calcolo delle sanzioni**
.

❝ *Il rinvio sui sistemi alto rischio è **confermato** — ma **tre tappe sono già esigibili** e l'Omnibus introduce **nuove priorità.***

Le nuove scadenze e cosa cambia per le aziende.

Le nuove scadenze · alto rischio rinviato, MA non tutto è rimandato

ANTICIPATA

2 dic 2026

Watermarking contenuti IA

Marcatura dei contenuti generati da IA per i **sistemi già sul mercato prima di agosto 2026**.

NUOVI DIVIETI

2 dic 2026

Deep fake pornografici

Divieto su IA che genera materiale **pornografico non consensuale** o **pedopornografico**.

↻ RINVIO ALTO RISCHIO

2 dic 2027

Stand-alone (Allegato III)

Applicazione obblighi alto rischio: **documentazione, log, supervisione umana**.

↻ RINVIO COMPONENTI

2 ago 2028

Componenti di sicurezza (All. I)

Sistemi alto rischio **integrati in prodotti regolamentati** (dispositivi medici, veicoli).

Cosa cambia operativamente per le aziende

01 SEMPLIFICAZIONI ESTESE

PMI + Small Mid-Caps

Le agevolazioni PMI sono **estese alle Small Mid-Caps — fino a 499 dipendenti**.

→ Meno oneri di registrazione sui sistemi meno rischiosi.

02 ART. 4 RINFORZATO

Alfabetizzazione: dal "garantire" al "sostenere"

Fornitori e deployer devono **"sostenere lo sviluppo"** dell'alfabetizzazione — non solo garantirla.

→ Obbligo **attivo e continuativo**.

03 GOVERNANCE CENTRALE

Ufficio europeo per l'IA

Competenza **esclusiva** su **GPAI** e **grandi piattaforme online (VLOP)**.

→ Stop alla frammentazione tra autorità nazionali.

Tempo guadagnato sull'alto rischio — non tempo per attendere, ma tempo per organizzarsi.

Livello italiano

La Legge italiana sull'IA — L. 132/2025.

Il livello nazionale **si aggiunge** al Regolamento UE — obblighi e fattispecie italiane.

01 PROFESSIONISTI

Trasparenza verso il cliente

Chi usa IA in attività professionale deve comunicare al cliente — **chiaro, semplice, esaustivo**:

- **Natura** del sistema
- **Finalità** d'uso
- **Grado di intervento umano**
- **Limitazioni** e **rischi**

→ Trasparenza = **autonomia del cliente** + **lealtà**.

02 ⚠ NUOVO REATO

Art. 612-quater c.p.

"Illecita diffusione di contenuti generati o manipolati con IA"

Reclusione da 1 a 5 anni

Per chi cagiona **danno ingiusto** diffondendo contenuti IA **idonei a ingannare**.

ELEMENTI COSTITUTIVI

- Generazione/manipolazione **via IA**
- **Diffusione**
- **Idoneità ingannatoria**
- **Danno ingiusto**

Procedibilità a querela (d'ufficio in casi tassativi).

03 AGGRAVANTE COMUNE

Art. 61 n. 11-decies c.p.

Uso dell'IA come fattore aggravante

Si applica quando il sistema di IA è usato:

- come **mezzo insidioso**
- come **ostacolo alla difesa** pubblica o privata
- come fattore che **aggrava le conseguenze** del reato

04 Diritto d'Autore (Art. 25)

LA TUTELA È RISERVATA ESCLUSIVAMENTE ALLE OPERE DELL'INGEGNO UMANO.

L'uso dell'IA come supporto è ammesso, ma la protezione scatta solo se l'opera finale costituisce il risultato del lavoro intellettuale dell'autore.

• Pausa · mettiamoci in gioco

The Game

Quanto sei davvero in regola?

Cinque domande. Cinque minuti.
Ora chiudiamo le slide.

Cosa intende l'AI Act quando parla di "sistema di IA".

DEFINIZIONE · ART. 3

Qualunque software che...

per obiettivi definiti dall'essere umano, **genera contenuti, previsioni, raccomandazioni o decisioni** in grado di influenzare l'ambiente fisico o virtuale.

> **Non solo** ML sofisticato. **Non solo** sistemi sviluppati internamente.

⚠ "Noi non sviluppiamo IA → l'AI Act non ci riguarda" — **è esattamente il contrario**.

Strumenti già coperti dal Regolamento

- **ChatGPT, Claude, Gemini** — LLM per testi aziendali
- **Microsoft 365 Copilot** — Sintesi documenti, riunioni
- **Screening CV (HR)** — Tool di ordinamento candidati
- **Chatbot, customer service** — FAQ automatizzate
- **Lead scoring sales** — Marketing predittivo
- **Manutenzione predittiva** — Stabilimenti, produzione
- **Image/video generation** — Campagne pubblicitarie
- **Analisi dati commerciali** — Forecast, scoring clienti

Mappare l'IA in azienda: il lato dati, non solo legale.

◉ INVENTARIO TECNICO

Cosa va censito davvero

- **Sistemi ufficiali** & SaaS aziendali: licenze, account, integrazioni
- **Shadow IT**: account personali, estensioni browser, plugin Office
- **Modelli embedded**: scoring in CRM/ERP/HRIS già attivi
- **Vendor che usano IA** sui tuoi dati senza dichiararlo
- **Modelli sperimentali**: POC, automazioni interne, script Python

↳ **Ogni voce** con: scopo d'uso, dati in input, dati in output, retention, fornitore, contratto.

○ DATA LINEAGE

Da dove vengono i dati che alimentano l'IA

Sorgenti → Modello IA → Decisione / Azione

3 domande tecniche da farsi su ogni nodo

01 Quali **categorie di dati personali** entrano nel modello?

02 I dati **escono dall'UE** o restano nel perimetro aziendale?

03 L'output del modello **produce decisioni** automatizzate su persone?

Senza mappa tecnica dei flussi, la documentazione legale è solo un esercizio di stile.

Art. 3 del Regolamento

I 4 ruoli nella catena del valore dell'IA.

Capire dove ti collochi è il punto da cui parte **ogni adempimento**. Ciascun ruolo ha obblighi propri.

RUOLO 1

Provider

Sviluppa un sistema di IA e lo immette sul mercato col proprio nome o marchio.

OBBLIGHI PIÙ STRINGENTI

- Valutazione conformità
- Documentazione tecnica
- Registrazione DB UE
- Marcatura CE
- Gestione del rischio

RUOLO 2

Deployer

Utilizza un sistema di IA **sotto la propria autorità** in ambito professionale.

OBBLIGHI ART. 26

- Uso conforme istruzioni
- Supervisione umana
- Monitoraggio
- Conservazione log
- Informativa interessati
- AI literacy (art. 4)

RUOLO 3

Importatore

Immette sul **mercato europeo** un sistema sviluppato da soggetto extra-UE.

Verifica che il provider extra-UE abbia rispettato gli obblighi.

RUOLO 4

Distributore

Mette a disposizione un sistema di IA sul mercato europeo **senza modificarne** le caratteristiche.

! **Passaggio critico:** il deployer può essere **riqualificato come provider** se modifica sostanzialmente il sistema o lo immette col proprio marchio.

Checklist a maggio 2026

Cosa è già obbligatorio oggi.

ART. 5 · DIVIETI

Pratiche vietate

Verificare che la tua azienda **non utilizzi neanche indirettamente** sistemi nei divieti: tecniche subliminali, sfruttamento di vulnerabilità, scoring sociale, riconoscimento emozioni lavoro/scuola, biometria sensibile.

FINO A 35M€ · 7%

ART. 4 · LITERACY

Alfabetizzazione AI

Mappare chi usa o interagisce con sistemi di IA — incluse marketing e HR — ed erogare **formazione adeguata al ruolo**. Documentata e mantenuta nel tempo.

ART. 50 · TRASPARENZA

Disclosure

I sistemi che interagiscono direttamente con persone devono essere **riconoscibili come tali**. Contenuti generati artificialmente: etichettatura nei modi previsti.

CAP. V · GPAI

Uso conforme

Se usi LLM forniti da terzi (GPT, Claude, Gemini), assicurati che **il provider abbia adempiuto** e che il tuo uso sia coerente con istruzioni e limitazioni.

+ GDPR

Pienamente applicabile

Ogni trattamento dati personali via IA: **base giuridica, informativa, registro, DPIA, responsabili esterni, trasferimenti extra-UE**.

Le

7

zone grigie

tipiche delle aziende italiane

COSA SONO

Situazioni in cui gli obblighi esistono già oggi.

Dai casi che vediamo ricorrere nei nostri assessment, abbiamo individuato **sette situazioni trasversali** alle aziende italiane di tutte le dimensioni.

9 volte su 10 nei primi screening: la maggior parte delle imprese è **di fatto fuori regola** — senza saperlo.

→ Le prossime due pagine le elencano una per una con il riferimento normativo.

⚡ **Tutte già pienamente esigibili a maggio 2026**

L'IA è già dentro la tua azienda — solo che non lo sai.

I numeri dello shadow AI

Quello che dicono **IDC, ISTAT, IBM, BCG, MIT, PagerDuty/Wakefield** sui dipendenti italiani ed europei nell'ultimo anno.

⚠ IL DATO PIÙ ECLATANTE

90%+

delle aziende — i lavoratori usano **strumenti di IA personali** senza alcuna supervisione aziendale.

MIT · 2025

ESPLOSIONE IN UN ANNO

DIPENDENTI CHE USANO GENAI

74% → 96%

In 12 mesi il **+22%** assoluto — la GenAI è entrata in azienda **prima delle policy**.

IBM · 2024

56%

dei dipendenti usa **strumenti AI non autorizzati** sul lavoro.

SHADOW IT

IDC · 2025

23%

soltanto usa strumenti AI **forniti e gestiti** dall'organizzazione.

GAP DI GOVERNANCE

IDC · 2025

38%

dei dipendenti ammette di **condividere dati sensibili** senza autorizzazione.

⚠ DATA LEAK

IBM · 2024

66%

degli impiegati ha usato strumenti AI **vietati dall'azienda**.

VIOLAZIONE POLICY

PagerDuty/Wakefield · 2025

53%

ha **continuato** a usare strumenti vietati anche **dopo** il primo richiamo formale.

RECIDIVI

PagerDuty · 2025

FOCUS ITALIA

67% usa regolarmente GenAI in settimana lavorativa · **54%** strumenti non autorizzati (**62% under 35**) · solo **19%** usa *esclusivamente* strumenti aziendali. — ISTAT · BCG · 2025

L'AI Act trova le aziende così.
Le 7 zone grigie nascono qui.

Zone grigie

Shadow IT, HR, marketing, chatbot.

01 ChatGPT, Copilot, Claude, Gemini senza policy aziendale

Il dipendente incolla bozze di contratti, dati clienti, prodotto. **Situazione più diffusa in assoluto.**

⚠ 3 RISCHI TECNICI SPESSO IGNORATI

Regurgitation — il modello riproduce testi protetti (caso *NYT vs OpenAI*) · **Allucinazioni** — citazioni/sentenze inesistenti (caso *Mata v. Avianca*) · **Perdita confidenzialità** — dati incollati possono finire nei dataset di training.

→ **Mitigazione:** policy d'uso + soluzioni **RAG** su perimetro controllato.

02 Screening CV e scoring nelle funzioni HR

Software che ordinano candidati o anche "solo" usare un LLM per **riassumere i CV ricevuti**.

⚠ ALTO RISCHIO · ALLEGATO III

03 Contenuti marketing IA senza disclosure

Immagini sintetiche, video con avatar, testi pubblicitari generati. **Quasi nessuna azienda italiana** li etichetta contro il rischio Deep Fake.

⚠ ART. 50 · ETICHETTATURA

04 Chatbot e assistenti virtuali su sito o app

L'utente va informato **in modo chiaro e tempestivo** che interagisce con IA, non con una persona.

⚠ ART. 50 · INFORMATIVA

Fornitori, sistemi predittivi, formazione.

05 Fornitori esterni che usano IA sui tuoi dati

L'agenzia che usa GPT-4 per le tue newsletter, il fornitore di customer service che gestisce le mail con IA.

⚠ EREDITI RISCHI NON CONTROLLATI

06 Sistemi predittivi già in produzione

Manutenzione predittiva, forecast, scoring rischio cliente. **Spesso integrati da anni**, senza mappa.

⚠ CLASSIFICAZIONE OBBLIGATORIA

07 Mancanza totale di formazione documentata sull'IA

ART. 4 · DAL 2 FEB 2025

Provider e deployer devono assicurare un **livello sufficiente di AI literacy** a chi sviluppa, usa, interagisce con i sistemi.

Non è formazione tecnica: è la capacità di **leggere criticamente** la tecnologia — riconoscerne i limiti, identificare bias, evitare la **dipendenza intellettuale**.

È **condizione di legittimità dell'uso stesso**: non un onere formale. Una sessione *"una tantum"* su "come usare ChatGPT" non assolve l'obbligo.

→ Delegare ogni ragionamento alla macchina **erode** nel tempo la capacità professionale autonoma.

La roadmap: 6 passi verso la conformità.

01 Mappatura

Sistemi di IA in uso + **shadow IT**. Inventario funzione per funzione, account personali, integrazioni informali.

02 Classificazione rischio

Inaccettabile, alto, limitato, minimo. **Con il ragionamento** documentato — in caso di controllo va dimostrato.

03 Analisi dei ruoli

Per ogni sistema: provider, deployer, importatore o distributore? **Per iscritto**.

04 Formazione (art. 4)

Percorsi **differenziati per ruolo**, valutazione finale, registro presenze, aggiornati nel tempo.

05 Policy & presidi

Policy d'uso, procedure approvazione, informative, registro sistemi, incident management, **DPIA**.

06 Governance fornitori

Revisione contratti, **clausole AI Act**, audit periodici sui provider esterni.

01 · Mappatura: senza inventario, niente conformità.

Sistemi di IA in uso **+ shadow IT**. Inventario funzione per funzione, account personali, integrazioni informali.

⚠ IL PUNTO DI PARTENZA

90%+

delle aziende ha lavoratori che usano **IA personale** senza supervisione.

20–40

sistemi attivi in media nelle PMI italiane (tra ufficiali, embedded, shadow IT).

▸ COSA CERCARE

Le 3 categorie da scovare

Sistemi ufficiali
Copilot, ChatGPT Enterprise, tool gestionali.

IA embedded
Già integrata in CRM, ERP, HR, marketing.

Shadow IT
Account personali, copia-incolla, browser plugin.

LE 3 DOMANDE

Per ogni sistema, provare a rispondere:

1 **Chi** lo usa e con quale frequenza?

2 **Quali dati** entrano nel sistema?

3 **Quali decisioni** influenzano l'output?

→ Output del passo 1: **registry vivo** (Notion / Airtable / DB).

⚠ L'ERRORE PIÙ COMUNE

"Noi non usiamo IA"

È la risposta più frequente **— ed è quasi sempre sbagliata**. L'IA è già nel tuo CRM, nelle email che scrivi, nei tool che usa il marketing. Non saperlo non è una scusante: è la prima zona grigia.

NORMA APPLICABILE

Art. 4 AI Act — alfabetizzazione e mappatura del personale che usa IA.

Art. 26 — obblighi del deployer su uso, monitoraggio, conservazione log.

Roadmap

02 · Classifica il rischio — e documenta il ragionamento.

Inaccettabile, alto, limitato, minimo. **Con il ragionamento documentato** — in caso di controllo va dimostrato.

RISCHIO MINIMO

Nessun obbligo specifico

Codici di condotta volontari.

Filtri antispam, traduzione automatica, suggerimenti musicali.

LIMITATO · ART. 50

Trasparenza

L'utente deve sapere di interagire con IA. Contenuti sintetici segnalati.

Chatbot, assistenti virtuali, deepfake, contenuti generati.

ALTO · ART. 6 + ALL. III

Conformità ex ante

Risk mgmt, qualità dati, log, supervisione umana (art. 14), robustezza.

HR, credito, sanità, istruzione, frontiere, dispositivi medici.

INACCETTABILE · ART. 5

Divieto assoluto

Sistemi vietati. Devi **verificare di non usarli neanche indirettamente**.

Social scoring, manipolazione, biometria real-time, riconoscimento emozioni a scuola/lavoro.

▸ COME SI DOCUMENTA

Per ogni sistema, una scheda di classificazione

- **Finalità d'uso** e contesto applicativo (settore, decisioni influenzate).
- **Verifica Allegato III**: rientra in una delle 8 aree alto rischio?
- **Esclusione** art. 5 (pratiche vietate) e art. 50 (trasparenza limitata).
- **Esito + motivazione**. Aggiornati a ogni modifica sostanziale.

⚠ ATTENZIONE PMI

HR + scoring credito = alto rischio

Lo screening CV e la valutazione lavoratori sono **esplicitamente classificati ad alto rischio** nell'Allegato III. Riguarda **quasi ogni PMI**.

03 · Per ogni sistema, qual è il tuo ruolo?

Provider, deployer, importatore o distributore. **Per iscritto** — i ruoli cambiano per sistema e nel tempo.

P **PROVIDER · ARTT. 16 ss.**

Chi sviluppa e immette

Risk mgmt, qualità dati, doc tecnica, valutazione conformità **ex ante**, banca dati UE, post-market.

Peso normativo **massimo**.

D **DEPLOYER · ARTT. 26 ss.**

Chi usa professionalmente

Uso conforme, supervisione **art. 14**, monitoraggio, log, informativa, cooperazione autorità.

← **TU sei qui** nella maggior parte dei casi.

I **IMPORTATORE**

Chi porta in UE

Verifica che il provider **extra-UE** abbia adempiuto. Conserva documentazione e marcatura CE.

Rivenditori IA **USA/UK**: spesso qui.

X **DISTRIBUTORE**

Chi rivende nella filiera

Verifica conformità prima della messa a disposizione. Sospende in caso di non-conformità.

SI consulting, MSP, system integrator.

⚠ **ATTENZIONE — DIVENTI PROVIDER SE...**

1. **Modifichi sostanzialmente** un sistema esistente.
2. Lo immetti sul mercato **col tuo marchio** (rebranding).
3. Cambi la **finalità d'uso** rispetto a quella dichiarata dal provider originario.

▸ **DELIVERABLE DEL PASSO 3**

Una **scheda ruolo** per ogni sistema della tua mappa, firmata e archiviata — con riferimento contrattuale al provider e indicazione di chi (in azienda) è **owner del rischio**.

Roadmap

04 · Formazione — già obbligatoria, raramente fatta bene.

Percorsi **differenziati per ruolo**, valutazione finale, registro presenze, aggiornati nel tempo.

⚡ ATTIVO DAL 2 FEB 2025

L'art. 4 non chiede "consapevolezza generica"

Chiede **AI Literacy proporzionata al ruolo, continuativa, verificabile**. L'Omnibus 2026 rinforza: si passa dal "garantire" al "sostenere lo sviluppo".

Percorsi differenziati — uno per ruolo

LEADERSHIP

Imprenditori, direttori

Cornice normativa, ruoli, sanzioni. **Decisioni di governance**, non operatività.

2-4 ore · annuale.

FUNZIONI ESPOSTE

HR, marketing, vendite

Casi d'uso, **limiti operativi**, etichettatura art. 50, divieto sistemi alto rischio non autorizzati.

Workshop pratici per funzione.

SUPERVISORI ART. 14

Chi supervisiona alto rischio

Logiche del modello, **distorsione automazione**, intervento e kill switch. **Formazione qualificata**.

Verifica finale obbligatoria.

IT, DPO, LEGAL

Owner della conformità

Logging, monitoraggio, FRIA, DPIA, contratti vendor, gestione incidenti.

Aggiornamento continuo.

✕ COSA NON È FORMAZIONE

- ✕ **Una sessione di 2 ore** per tutti, una tantum.
- ✕ **Un PDF girato via email** con riepilogo della normativa.
- ✕ **"Come usare ChatGPT"** — è un tutorial, non AI Literacy.

IL TEMA CHE MANCA

Dipendenza intellettuale

Delegare ogni ragionamento alla macchina **erode la capacità autonoma**. Va prevenuta in formazione — non è solo un'opinione, è AI Literacy.

Roadmap

05 · Policy & presidi — la conformità diventa sistema vivo.

Policy d'uso, procedure di approvazione, informative, registro sistemi, incident management, **DPIA**.

01 Policy d'uso aziendale

Cosa è ammesso, cosa è vietato, quali dati **non possono uscire**. Linguaggio operativo, esempi concreti.

02 Procedura di approvazione

Chi autorizza un nuovo sistema IA. **Check normativo + tecnico** prima del rollout. Niente "ce l'ho già scaricato".

03 Sorveglianza umana art. 14

Persona competente con **autorità reale di intervento**. Comprensione, vigilanza, kill switch documentati.

04 Logging & tracciabilità

Log di inferenze, prompt, output. **Almeno 6 mesi** per l'alto rischio (art. 26). Non è backup — è audit trail.

05 DPIA + FRIA

DPIA per dati personali (GDPR) · **FRIA** per impatti sui diritti (AI Act). Atti sostanziali, non formali.

06 Incident management

Procedure di segnalazione e notifica. **72 ore** per i data breach (GDPR), incidenti gravi all'autorità AI (AI Act).

IL PRINCIPIO

Le policy le scrivi una volta. I sistemi vivono ogni giorno.

Una policy senza presidi tecnici è un foglio firmato. **I 6 elementi devono lavorare insieme** per costituire conformità documentabile.

⚠ DOVE SONO LE PMI

Oggi **9 PMI italiane su 10** sono ferme tra **L0 (caos)** e **L1 (policy scritta, niente vivo)**.

06 · Governance fornitori — chiude la filiera.

Revisione contratti, **clausole AI Act**, audit periodici sui provider esterni. La tua compliance dipende anche dalla loro.

IL PRINCIPIO Il regime **GPAI non sostituisce** gli obblighi del deployer: li condiziona. **Documentare** la compliance del provider è parte della tua due diligence.

▸ COSA FARE — 4 AZIONI

Sui contratti con i fornitori IA

1. **Verifica adempimento del provider**
   Documentazione tecnica, codici di condotta GPAI, dichiarazione di conformità. **Per iscritto**.

2. **Clausole AI Act in contratto**
   Limitazioni d'uso, finalità ammesse, cooperazione su audit/incidenti, gestione dei dati di training. In attesa delle **MCC-AI** della Commissione.

3. **Audit periodici**
   Rivisita annualmente lo stato di compliance del provider. **Soprattutto per fornitori extra-UE**.

4. **Rispetta le istruzioni d'uso**
   Limitazioni e finalità dichiarate dal provider sono **vincolanti** — se le violi, esci dalla copertura della loro compliance.

⚠ RED FLAG — DIVENTI PROVIDER

Modifichi, rinomini, ricontestualizzi?

Se **modifichi sostanzialmente**, **cambi il marchio** o **la finalità d'uso** di un sistema, l'AI Act ti tratta come provider — con tutti gli obblighi ex-ante.

→ Tipico in MSP, system integrator, prodotti white-label.

▸ DUE DILIGENCE — DA CHIEDERE PER ISCRITTO

- ✓ **Documentazione tecnica** e politica copyright UE
- ✓ **Sintesi pubblica** dei dati di training
- ✓ **Adesione al Codice di condotta GPAI** (lug 2025)
- ✓ **DPA** + trasferimenti extra-UE conformi GDPR

I 5 errori più frequenti

Cosa NON fare.

Sei comportamenti che espongono le aziende italiane a **rischi concreti**.

Aspettare la conferma delle scadenze prima di muoversi

Gli obblighi già in vigore sono **numerosi e sostanziosi**; il rinvio eventuale riguarda solo una parte del Regolamento.

Affidarsi a modelli scaricati da internet

Policy generiche e informative copia-incollate non reggono a un controllo: **la conformità è specifica, non astratta**.

Trattare la conformità come tema esclusivamente legale

L'AI Act è una norma di governance: **investe legal, IT, HR, marketing, operations**. Senza coordinamento i progetti si arenano.

Erogare una formazione "una tantum"

L'alfabetizzazione AI è **continua** e va aggiornata con l'evoluzione dei sistemi e delle norme.

Sottovalutare la dipendenza intellettuale dall'IA

Delegare alla macchina ogni ragionamento erode nel tempo la capacità professionale autonoma. Chi non sa più **valutare criticamente l'output** non è in grado di intercettarne gli errori (allucinazione, bias).

Pensare che l'uso di strumenti consumer (ChatGPT, Gemini, Claude free) sia "invisibile"

Lo shadow IT è oggi il primo fattore di rischio. Le autorità lo sanno, e qualunque audit serio parte da lì.

Il prossimo passo

Pre-assessment AI Act gratuito.

Una fotografia operativa del livello di esposizione della tua azienda.

STEP 1 · LA SESSIONE

30-45 min in videocall

Questionario operativo: sistemi, ruoli, dati, formazione, policy.

STEP 2 · IL RISULTATO

Mini-report entro 48 ore

Livello esposizione + 3 rischi prioritari + 3 azioni urgenti.

STEP 3 · CONDIZIONI

Prima sessione gratuita

Una diagnosi accurata è il presupposto di qualsiasi intervento successivo: preferiamo offrirla, non venderla.

28 · Documento informativo

Riferimenti normativi e disclaimer.

FONTI NORMATIVE

Riferimenti

- **Reg. (UE) 2024/1689 — AI Act** · Parlamento e Consiglio UE
- **Reg. (UE) 2016/679 — GDPR**
- **Legge italiana 132/2025** · disposizioni in materia di IA
- **Linee guida UE 2019 — AI HLEG** · 7 requisiti IA affidabile
- **Linee guida del Garante** · protezione dati personali
- **Codice di condotta GPAI** · Commissione UE · luglio 2025
- **Codice trasparenza contenuti IA** · 2026
- **Carta HOROS** · Ordine Avvocati Milano · dic 2024
- **Linee guida CCBE 2024** · Consiglio Ordini Forensi Europei

⚠ DISCLAIMER

Avvertenze d'uso

Documento **informativo aggiornato a giugno 2026**. Non sostituisce una **consulenza professionale specifica**: il rischio reale dipende da settore, sistemi in uso, dati trattati e ruoli ricoperti.

La normativa è in evoluzione. L'**Omnibus Digitale** (approvato il 16 giugno 2026) ha confermato il rinvio dei sistemi ad alto rischio al 2 dicembre 2027 / 2 agosto 2028 e introdotto nuovi divieti immediati.

29 Giugno 2026
A cura di Avv. Pierluigi Spera e Antonio Alaia.

avvocatospera.it · namidi.it

Grazie!

Domande?

Grazie per l'attenzione, per il tempo,
per **aver letto fino in fondo**.

Lato giuridico

Avv. Pierluigi Spera

pierluigi.spera@sphera.legal

Lato dati & tecnico

Antonio Alaia

a.alaia@namidi.it