PARTNER 24ORE NETWORK

AI Responsabile in azienda: opportunità, rischi e governance

27 Ottobre 2025

tinexta cyber

think next,
secure now

INDICE

- ✓ L’Intelligenza artificiale
  1. Quadro Normativo Europeo e Italiano sull’Intelligenza Artificiale
  2. Cos’è l’AI realmente
  3. Come governare l’AI nei processi aziendali
  4. Utilizzo controllato e consapevole
  6. Il Codice Etico nell’AI
  7. Formazione, misura di sicurezza prodromica
  8. What’s Next

tinexta cyber

think next, secure now

Cosa prevede il Quadro normativo Europeo e Italiano sull'Intelligenza Artificiale?

tinexta
cyber

AI Act - REGOLAMENTO (UE) 2024/1689

AI ACT

- Primo quadro regolatorio armonizzato dell'Unione Europea in tema di intelligenza artificiale, volto a promuovere uno sviluppo dell'IA affidabile, sicuro e rispettoso dei diritti fondamentali
- Approccio basato sul rischio ("risk-based approach") che suddivide i sistemi di IA in categorie, in funzione del livello di rischio per la salute, la sicurezza o i diritti fondamentali
- Divieti assoluti per pratiche considerate a "rischio inaccettabile" (es. social scoring generalizzato, manipolazione comportamentale, biometria in spazi pubblici senza salvaguardie)
- Regole dettagliate per i "sistemi ad alto rischio" (high-risk AI systems), con obblighi di gestione del rischio, trasparenza, log, controllo umano, robustezza, qualità dei dati, registrazione, valutazione di conformità
- Obblighi per i modelli di uso generale (GPAI) e per il mercato, con regole specifiche per chiunque sviluppi, distribuisca, importi o impieghi sistemi IA
- Si applica anche a fornitori non-UE se il sistema è messo a disposizione o i risultati sono utilizzati nell'UE (Ambito di applicazione extraterritoriale)
- Sanzioni elevate (fino a 35 milioni di euro o il 7 % del fatturato globale) per le pratiche vietate
- Pubblicato 12 luglio 2024, in vigore dall'1 agosto 2024, con disposizioni operative progressivamente (alcune dal 2 febbraio 2025, altre dal 2 agosto 2026 o 2027, secondo cronoprogramma)
- Obiettivo complessivo: creare un "ecosistema europeo" dell'IA che favorisca anche l'innovazione, la competitività e l'affidabilità

Legge n. 132 del 23 settembre 2025

Legge italiana sull'AI

- Normativa nazionale italiana che entra in vigore il 10 ottobre 2025.
- Finalizzata a integrare e attuare a livello nazionale il quadro dell'UE (AI Act) ma con specifiche disposizioni italiane per alcuni settori sensibili (lavoro, sanità, ricerca, pubblica amministrazione) e con un'attenzione accentuata alla tutela dei diritti, trasparenza, supervisione e formazione.
- Obbligo per i datori di lavoro di informare i dipendenti quando è impiegato un sistema di IA nei processi lavorativi; trasparenza su logica, dati, parametri, metriche, supervisione umana; valutazione di impatto; coinvolgimento sindacale.
- In sanità: obblighi di informazione al paziente quando IA è usata nella cura; divieto di discriminazione; standard di affidabilità; controlli periodici.
- Per la ricerca sanitaria e l'uso secondario dei dati pseudonimizzati vige la previsione di notifica al Garante per la protezione dei dati personali con DPIA e misure di sicurezza; uso di anonimizzazione / pseudonimizzazione / dati sintetici.
- Introduzione di nuovi reati/illeciti per l'uso illecito di IA (es. deepfake, Text Data Mining non autorizzato) e misure di contrasto.
- Si affianca all'AI Act, ma consente all'Italia di modulare l'applicazione in base al contesto nazionale, e di anticipare aspetti settoriali prima dell'entrata piena in vigore della regolamentazione UE.

Tabella comparativa

Tema	AI Act (UE)	Legge 132/2025 (Italia)	Differenze / novità chiave
Ambito normativo	Regolazione europea orizzontale che disciplina tutti i sistemi IA nell'UE (e in certi casi fuori) con approccio generale.	Normativa nazionale italiana che implementa ed integra il quadro UE, con attenzione settoriale e nazionale.	L'Italia anticipa/dispone una legge nazionale che si integra con il regolamento UE ma con specifiche nazionali (es. lavoro, sanità).
Approccio al rischio	Classifica i sistemi IA in base al rischio (inaccettabile, alto rischio, rischio limitato, minimo).	Prevede obblighi specifici per settori sensibili (lavoro, sanità, ricerca) ma non esattamente la stessa articolazione "alto-rischio" vs "basso rischio".	La legge nazionale applica i principi UE ma li declina con specificità per il contesto italiano.
Divieti / Pratiche vietate	Elenco di pratiche vietate (social scoring, manipolazione, biometria senza salvaguardie) sotto "rischio inaccettabile".	Prevede reati specifici per uso illecito dell'IA (deepfake, TDM - >Text Data Mining -non autorizzato), con sanzioni penali	L'Italia introduce profili penali più espliciti e adatta al proprio ordinamento giudiziario.
Obblighi per "alto rischio" IA	Obblighi rigorosi per i provider/deployer di sistemi ad alto rischio: risk management, qualità dati, log, supervisione umana, conformità, marcatura CE, Post Market Surveillance (PMS), registrazione.	Pur richiedendo trasparenza e obblighi settoriali, la legge italiana si concentra in gran parte su lavoro, sanità, ricerca e su informazione, supervisione, DPIA, non tanto sull'intero ciclo "alto rischio" come nel testo UE.	Il testo UE è più strutturato per "alto rischio" in senso tecnico-prodotto; quello italiano privilegia settori d'uso e protezione dei diritti.
Trasparenza / informazione	Trasparenza nei sistemi IA: obbligo di informare che si interagisce con un'IA, etichettatura di contenuti sintetici, log, documentazione tecnica.	Obbligo nazionale di informare lavoratori/pazienti quando IA è usata, trasparenza su logica, parametri, metriche, dati/uso, coinvolgimento sindacati.	La legge italiana richiede dettagli operativi di trasparenza nel contesto lavoro/health, andando oltre solo la "etichettatura".
Ambito settoriale e nazionale	Uniforme per tutti gli Stati membri, a prescindere dal settore; segue un approccio cross-sector.	Specifica disposizioni per lavoro, sanità, ricerca, pubblica amministrazione, con potere delegato al governo per decreti attuativi.	L'Italia applica l'orizzonte UE ma consente disciplina settoriale interna addizionale.
Tempistica / entrata in vigore	In vigore dal 1 agosto 2024, ma obblighi operativi scaglionati (alcuni dal 2 feb 2025, altri dal 2 ago 2026/2027)	Entra in vigore il 10 ottobre 2025; alcuni obblighi attuativi richiedono decreti delegati entro 12 mesi.	L'Italia anticipa l'entrata del suo quadro nazionale, ma l'applicazione completa del regolamento UE resta successive.
Sanzioni / responsabilità	Sanzioni pecuniarie molto elevate (es. fino a €35 milioni o 7% fatturato globale) per violazioni gravi.	Prevede sanzioni amministrative e penali: reclusione per deepfake illecito, sanzioni specifiche; dettagli da decreti attuativi.	Il regime sanzionatorio italiano aggiunge profili penali settoriali, mentre quello UE è centrato su sanzioni pecuniarie per operatori.
Innovazione e competitività	Promuove creazione dell'ecosistema europeo di IA, test environment, supporto a start-up; bilanciamento tra innovazione e regolamentazione.	La legge italiana include misure per supporto all'innovazione nazionale (es. fondi, venture) e disciplina nazionale anticipata.	Pur condividendo la finalità di supportare innovazione, la legge italiana sottolinea anche la sovranità tecnologica nazionale.

- **Pratiche vietate e alfabetizzazione AI: applicabili dal 2/2/2025**
- **Obblighi GPAI: dal 2/8/2025**
- **Obblighi sistemi ad alto rischio (Annex III): dal 2/8/2026**
- **High-risk embedded in prodotti regolati: fino al 2/8/2027**

tinexta cyber

IA Pubblica e Privata: due modelli di servizio a confronto

Sistema di IA Pubblico

Modello:

- Utilizza un sistema di IA disponibile pubblicamente, che beneficia di più utenti a livello globale che inseriscono dati, i quali possono essere usati per addestrare ulteriormente il modello.
- Comporta un rischio significativo di esposizione accidentale dei dati e output di bassa qualità che compromettono l'integrità dei dati.
- Il rischio di attacco al sistema di IA è gestito dal fornitore e non dall'utente.

Sistema di IA Privato

Modello:

- Sistema privato usato solo all'interno dell'organizzazione che lo possiede.
- I rischi di riservatezza e privacy dei dati sono minori, ma comunque presenti (es. dati personali usati nell'addestramento).
- Gli output devono essere verificati per la qualità prima di essere utilizzati nei processi aziendali, per prevenire problemi di integrità dei dati.
- Il proprietario del sistema si assume i rischi di attacco.

Differenti tipologie di AI

Evoluzione dell'AI

Machine Learning

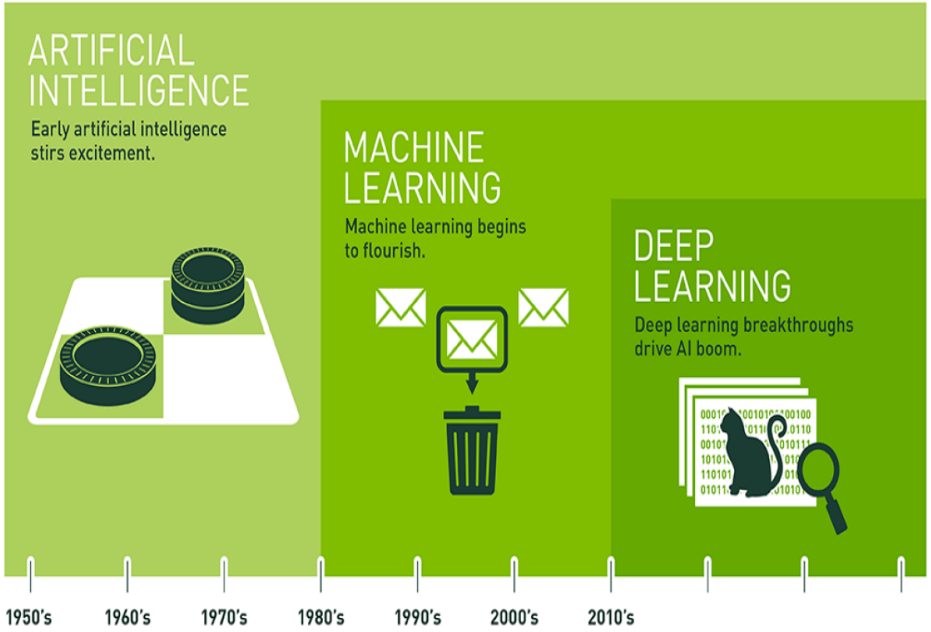
È la tecnologia che consente ai sistemi di imparare dai dati e migliorare nel tempo senza essere programmati in modo esplicito. Viene usata, ad esempio, per prevedere vendite, analizzare comportamenti o riconoscere modelli nei dati.

Deep Learning

È una forma avanzata di machine learning che usa reti neurali artificiali con molti strati per riconoscere schemi complessi, come immagini, voce o testo. È alla base di sistemi come il riconoscimento di forme, oggetti fino al riconoscimento facciale e traduzione automatica.

AI Generativa

È l'AI che crea nuovi contenuti ispirandosi ai dati su cui è stata addestrata (testi, immagini, suoni o video, replicando stili e strutture appresi). Esempi noti sono ChatGPT, DALL·E, CLAUDE, e altri modelli capaci di generare contenuti originali.



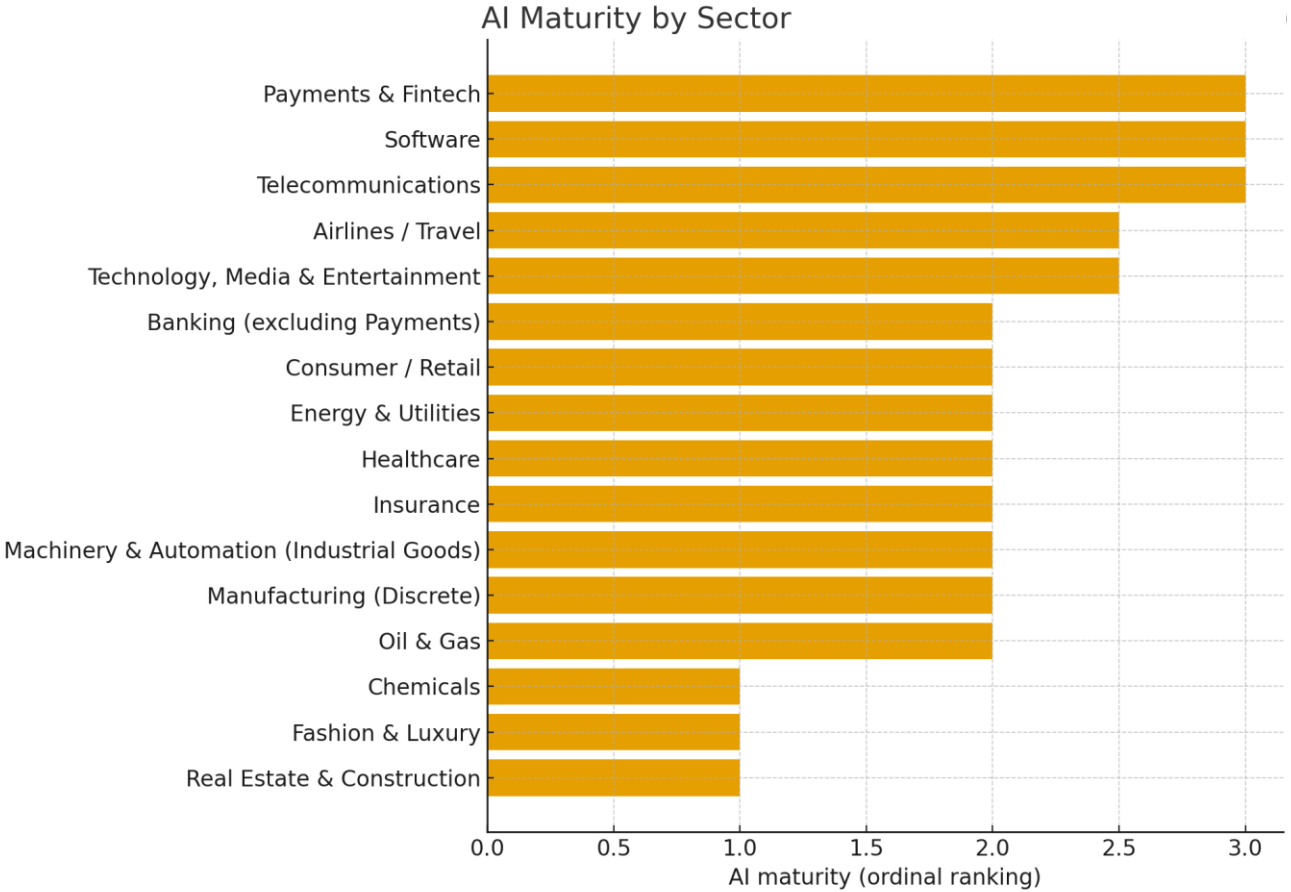
Since an early flush of optimism in the 1950s, smaller subsets of artificial intelligence – first machine learning, then deep learning, a subset of machine learning – have created ever larger disruptions.

tinexta cyber

Principali rischi legati all'uso dell'IA

Rischio	Descrizione
Accuratezza e affidabilità	Le soluzioni generative possono **produrre risposte errate, inventate o fuorvianti,** e non hanno garanzia di validità o completezza
Privacy, dati e sicurezza	Vi è il pericolo che dati personali o sensibili vengano **esposti, riutilizzati o inseriti senza consapevolezza**, e che l'IA stessa venga usata per attacchi o sfruttata da malintenzionati
Bias, discriminazione ed etica	I modelli possono riflettere o amplificare **pregiudizi impliciti** nei dati di addestramento, generando risultati ingiusti o stereotipati
Aspetti legali, regolamentari e proprietà intellettuale	Ci sono questioni complesse su **chi detiene i diritti** del contenuto generato, su come vengono usati dati protetti, e potenziali sanzioni per mancata conformità
Manipolazione, disinformazione e impatti sociali	L'IA generativa può **produrre contenuti realistici falsi o manipolativi** (deepfake, disinformazione), con conseguenze su opinione pubblica, reputazione e fiducia
Rischi operativi e organizzativi	Nell'adozione aziendale, **mancanza di governance, ruoli poco chiari, supervisione insufficiente** possono creare vulnerabilità e inefficienze
Impatti ambientali e di sostenibilità	L'addestramento e l'esecuzione massiva di modelli generativi richiedono **grandi risorse energetiche, acqua, hardware**, con impatti ambientali importanti

AI Maturity Benchmark



tinexta cyber

Matrice obblighi, azioni, scadenze, sanzioni

Obbligo	Azione da implementare	Owner aziendale	Deadline	Sanzioni
AI Act – Pratiche vietate (unacceptable risk)	Eseguire gap assessment su tutti i casi d'uso; cessare/evitare pratiche vietate (es. social scoring, manipolazione dannosa, scraping biometrico massivo). Integrare controllo pre-rilascio.	Legal/Compliance, IT Security, Product	Applicabile dal 2 Feb 2025; continuo	Fino a €35M o 7% fatturato globale (art. 99)
AI Act – Obblighi per GPAI (modelli di uso generale)	Implementare sintesi pubblica dei dati di training; processi per copyright/opt-out; valutazione e mitigazione rischi di modello; notifica ad AI Office se 'systemic risk'.	AI/ML, Legal IP, Data Governance	Dal 2 Ago 2025	Fino a €15M o 3% (altre violazioni); €7,5M o 1% per info inesatte
AI Act – Trasparenza contenuti sintetici / deepfake	Etichettare contenuti generati (deepfake) in modo chiaro e visibile; informare quando l'utente interagisce con un sistema AI (chatbot)	Communications/User Experience, Product, Legal	Regola generale dal 2 Ago 2026	Fino a €15M o 3% (inadempienze)
AI Act – Provider sistemi ad alto rischio (Annex III)	Sistema di risk management; governance dati; documentazione tecnica; logging; istruzioni all'utilizzatore; human oversight; robustezza /cybersecurity/accuracy; registrazione EU DB (Banca dati europea); valutazione di conformità e marcatura CE; PMS (Post Market Surveillance) & incident reporting.	AI/ML, QA/Regulatory, Security, Legal/Compliance	Dal 2 Ago 2026 (Annex III)	Fino a €15M o 3%; €7,5M o 1% per info inesatte
AI Act – High-risk embedded in prodotti regolati	Coordinare con regolamenti di settore (Medical Device Regulation/In Vitro Diagnostic Regulatio, ecc.). Pianificare iter con organismi notificati e adeguare QMS.	RA/QA, Product, Legal	Proroga fino al 2 Ago 2027	Fino a €15M o 3%
AI Act – Deployers (utilizzatori) di sistemi ad alto rischio	Usare secondo istruzioni; assegnare supervisione umana; garantire qualità input; conservare log ≥6 mesi; informare i lavoratori prima dell'uso; monitorare e segnalare incidenti seri.	Funzione di Business owner del caso d'uso, HR (se personale), IT Ops, Compliance	Dal 2 Ago 2026	Fino a €15M o 3%; €7,5M o 1% per info inesatte
Legge 132/2025 – Lavoro	Informare i dipendenti sull'uso di AI nei processi; trasparenza su logica, scopi, dati/parametri, metriche (accuracy/robustness/cybersecurity), meccanismi di controllo umano; svolgere valutazioni d'impatto; coinvolgere sindacati ove previsto; promuovere formazione.	HR, Legal/Compliance, DPO, IT/AI Governance	In vigore dal 10 Ott 2025	Sanzioni definite anche via decreti delegati; possibili ispezioni Autorità
Legge 132/2025 – Sanità (uso clinico)	Informare i pazienti quando è usata AI; adottare standard di affidabilità; verifiche periodiche e aggiornamenti; progettare per minimizzare il rischio; divieto di discriminazione nell'accesso ai servizi.	Direzione Sanitaria, Risk Management, CIO/Clinical Engineering, Legal	In vigore dal 10 Ott 2025	Responsabilità professionale; sanzioni/amministrative settoriali (decreti)
Legge 132/2025 – Ricerca sanitaria / dati	Per uso secondario di dati pseudonimizzati: notificare il Garante con DPIA e misure di sicurezza; attendere 30 gg (silenzio-assenso salvo blocco). Ammesse anonimizzazione/pseudonimizzazione/synthetic data.	R&D, DPO, Data Governance	In vigore dal 10 Ott 2025 (per ogni progetto)	Inadempienze soggette a provvedimenti Garante e sanzioni secondo GDPR/attuativi
Legge 132/2025 – Reati (deepfake, TDM)	Prevenire e vietare la diffusione illecita di contenuti AI-manipolati; governare text-and-data mining nel rispetto del diritto d'autore; aggiornare policy interne e controlli.	Legal/Compliance, IP, Security, Comms	In vigore dal 10 Ott 2025	Reato di diffusione illecita di deepfake: reclusione 1–5 anni; aggravanti per reati commessi con AI; reato di TDM non autorizzato.
Legge 132/2025 – Decreti attuativi (12 mesi)	Monitorare decreti delegati su sanzioni/settori (finanza, assicurazioni, PA, giustizia, lavoro, media); predisporre gap analysis e piano di adeguamento.	Public Policy/Regulatory Affairs, Legal	Entro 12 mesi dall'entrata in vigore (entro Ott 2026)	Nuovo sistema sanzionatorio nazionale atteso (in aggiunta all'AI Act)

Cos’è davvero l’Intelligenza Artificiale?

La mente digitale del nostro tempo

tinexta
cyber

Categorie di rischio

RISCHIO INACCETTABILE

I Sistemi di IA considerati contrari ai valori fondamentali dell'UE e vietati, non sono ammessi sul mercato né nell'uso in UE

- Social scoring governativo o aziendale basato su comportamento o status sociale
- Manipolazione cognitiva o comportamentale che causa danno (es. giocattoli che influenzano i minori)
- Identificazione biometrica remota in tempo reale in spazi pubblici (salvo eccezioni di sicurezza)
- Riconoscimento emozionale coercitivo nei luoghi di lavoro o nelle scuole

RISCHIO ALTO

I Sistemi di IA che possono incidere in modo significativo su sicurezza, diritti o libertà delle persone, sono soggetti a requisiti tecnici e procedurali stringenti (risk management, qualità dati, logging, supervisione umana, marcatura CE)

- Sistemi di IA usati in selezione del personale o valutazione performance lavorativa
- Algoritmi di scoring creditizio o assicurativo
- Dispositivi medici con componenti di IA diagnostica
- Sistemi di giustizia predittiva o accesso a servizi pubblici
- Sistemi di sorveglianza o sicurezza critici

RISCHIO LIMITATO

I Sistemi di IA che comportano un rischio moderato, principalmente connesso alla trasparenza verso l'utente, richiedono di informare chiaramente l'utente che sta interagendo con un sistema di IA

- Chatbot e assistenti virtuali
- Sistemi di raccomandazione (es. piattaforme e-commerce o streaming)
- Generatori di contenuti testuali o grafici (deepfake) con obbligo di etichettatura
- Sistemi di sintesi vocale automatica

RISCHIO MINIMO O NULLO

I Sistemi di IA a basso impatto sui diritti o la sicurezza, non prevedono obblighi specifici oltre al rispetto generale della normativa UE

- Filtri antispam
- Giochi con IA integrata
- App di traduzione automatica o correzione ortografica
- Funzionalità AI non decisive per la sicurezza o i diritti delle persone

L'AI Act adotta un **approccio basato sul rischio** e distingue **quattro categorie** di rischio.
Ogni livello comporta **obblighi diversi per sviluppatori, distributori e utilizzatori** dei sistemi di intelligenza artificiale.

tinexta cyber

Criticità

PRIVATE

Area	Criticità	Impatto pratico
Identificazione dei sistemi AI “ad alto rischio”	Molte aziende non sanno se i propri algoritmi o servizi rientrano tra quelli classificati “high-risk” (Annex III). I criteri sono tecnici e interpretativi (es. “influenza significativa su diritti o sicurezza”).	Incertezza su chi debba attuare marcatura CE, valutazioni di conformità e registrazioni. Rischio di sotto-o-sovra-compliance.
Costi e complessità di conformità	Implementare processi di risk management, logging, tracciabilità dei dati e human oversight è oneroso, specie per PMI e start-up.	Rischio di frenare l’innovazione o spostare R&D fuori UE. Serve supporto economico e linee guida pratiche.
Responsabilità contrattuale e di filiera	L’AI Act coinvolge provider, importatori, distributori, deployer: la catena di responsabilità è complessa e poco allineata ai contratti tipici (SaaS, API, outsourcing).	Necessità di rinegoziare contratti e SLA; rischio legale condiviso tra più attori.
Data governance e copyright	Obblighi GPAI su trasparenza dataset e diritti d’autore difficili da implementare per modelli “black-box” o addestrati su fonti miste.	Esposizione a contestazioni Intellectual Property e Garante privacy; difficile dimostrare provenienza dei dati.
Trasparenza verso utenti e dipendenti	Obbligo di informare quando l’utente interagisce con un sistema AI o è valutato da esso (es. HR, credito).	Rischio di “pigrizia informativa” o di violare la privacy nel tentativo di essere trasparenti.
Coordinamento con GDPR e sicurezza	Doppio regime normativo (GDPR + AI Act) con requisiti sovrapposti ma non sempre coerenti (es. DPIA vs risk management AI).	Necessità di governance integrata (Legal + DPO + AI Governance + Security).
Sanzioni elevate e incertezza interpretativa	Pene fino al 7 % del fatturato globale per pratiche vietate.	Clima di prudenza eccessiva o blocco di progetti innovativi.

P.A.

Area	Criticità	Impatto pratico
Inventario dei sistemi AI in uso	Molte amministrazioni non hanno una mappatura dei sistemi IA (spesso embedded in software o forniti da terzi).	Difficoltà nel valutare rischio e conformità; rischio di uso “inconsapevole” di sistemi ad alto rischio.
Capacità tecnica e risorse	Scarsa disponibilità di competenze interne per audit, risk management e human oversight dei sistemi AI.	Dipendenza da fornitori esterni e tempi lunghi per adeguamento.
Bilanciamento innovazione / garanzie dei diritti	Nella PA l’uso di IA (es. nel welfare, giustizia predittiva, sanità) tocca diritti fondamentali, ma la normativa impone limiti stringenti.	Necessità di processi trasparenti e verificabili: rischio di rallentamento decisionale e blocco di sperimentazioni.
Trasparenza e accountability	La Legge 132/2025 impone obblighi di informazione verso cittadini e lavoratori pubblici, ma non chiarisce come applicarli nei sistemi pre-esistenti.	Rischio di frammentazione tra enti, mancanza di modelli standard di comunicazione.
Coordinamento tra autorità	AI Office UE, Garante Privacy, AGID, Ministeri, Autorità settoriali: molteplici soggetti competenti con ruoli non sempre chiari.	Sovrapposizioni e lentezza nel rilascio di linee guida nazionali.
Procurement e clausole contrattuali	Le gare pubbliche raramente includono requisiti di conformità AI Act o controlli ex-ante.	Necessità di aggiornare bandi e capitolati tecnici (pena rischio di non conformità).
Protezione dei dati e sorveglianza	L’uso di IA per biometria o videosorveglianza deve rispettare limiti strettissimi, ma spesso è già diffuso.	Potenziale blocco di strumenti di sicurezza non conformi.

tinexta cyber

Sistemi ad alto rischio

La gestione efficace delle criticità richiede una governance AI integrata, basata su competenze multidisciplinari (legali, tecniche e organizzative) e su un approccio proporzionato al rischio

Categoria (Allegato III)	Descrizione	Esempi pratici	Principali obblighi di conformità	Scadenza applicazione	Funzione / Owner aziendale
1. Identificazione biometrica e categorizzazione delle persone fisiche	Sistemi di IA che riconoscono o classificano persone tramite dati biometrici o comportamentali.	• Riconoscimento facciale per accessi o sorveglianza • Analisi emozioni nei luoghi di lavoro • Onboarding digitale con verifica identità	Valutazione rischio, trasparenza, accuratezza, supervisione umana, limitazione uso pubblico.	2 agosto 2026	IT Security, Privacy/DPO, Legal Compliance
2. Gestione e funzionamento di infrastrutture critiche	IA che incide su infrastrutture essenziali (energia, trasporti, acqua, telecomunicazioni).	• Controllo reti elettriche o idriche • Regolazione traffico ferroviario o aereo • Monitoraggio ponti o dighe	Gestione rischio, robustezza tecnica, audit log, cybersecurity, piani emergenza.	2 agosto 2026	Operations, Safety, IT Security, Engineering
3. Educazione e formazione professionale	Sistemi usati per valutare studenti o decidere accesso a percorsi formativi.	• Correzione automatica test • Selezione automatizzata borse di studio • Adaptive learning	Qualità dati, trasparenza, supervisione umana, prevenzione bias/discriminazioni.	2 agosto 2026	HR Training, Compliance, IT Governance
4. Occupazione, gestione dei lavoratori e accesso al lavoro autonomo	IA che incide su assunzione, performance, promozione o licenziamento.	• Screening CV • HR analytics • Assegnazione automatica turni	Trasparenza verso lavoratori, supervisione umana, logging, documentazione tecnica.	2 agosto 2026	HR, Legal, DPO, IT
5. Accesso e fruizione di servizi pubblici e privati essenziali	Sistemi che influenzano l'accesso a beni o servizi fondamentali (credito, salute, welfare).	• Credit scoring bancario • Sistemi di triage sanitario • Algoritmi per benefici sociali	Gestione rischio, qualità dati, spiegabilità decisioni, monitoraggio continuo.	2 agosto 2026	Risk Management, Compliance, Product Owner
6. Applicazione della legge (Law Enforcement)	IA usata per indagini, prevenzione o analisi attività criminali.	• Predictive policing • Analisi rischio recidiva • Videosorveglianza intelligente	Uso proporzionato, convalida legale, supervisione umana, logging, audit indipendente.	2 agosto 2026	Public Security, Legal, Data Governance
7. Gestione migrazione, asilo e controllo frontiere	IA che supporta decisioni su ingresso o espulsione nel territorio UE.	• Analisi automatica documenti • Biometria ai valichi • Analisi predittiva sicurezza	Trasparenza, supervisione, audit periodici, garanzie non discriminazione.	2 agosto 2026	Ministero Interno, Legal, IT Governance
8. Amministrazione della giustizia e processi democratici	IA usata per supportare decisioni giudiziarie o processi pubblici che incidono sui diritti.	• Analisi giurisprudenza • Assegnazione automatica fascicoli • Giustizia predittiva	Supervisione umana, trasparenza algoritmica, documentazione tecnica, audit regolare.	2 agosto 2026	Giustizia, IT Governance, Legal, Ethics Board

Responsabilità giuridiche in ambito AI

Livello di rischio / tipo di uso	Responsabilità della persona fisica	Responsabilità dell'azienda o ente	Riferimenti e note
🟥 **Rischio inaccettabile** **(pratiche vietate: social scoring, manipolazione cognitiva, sorveglianza biometrica indiscriminata)**	- Responsabilità penale diretta se partecipa alla progettazione, diffusione o utilizzo consapevole del sistema vietato. - Può configurarsi reato di trattamento illecito di dati, manipolazione o diffusione abusiva di contenuti (art. 132/2025, art. 167 ss. GDPR).	- Responsabilità amministrativa e penale dell'ente (D.Lgs. 231/2001) se l'uso deriva da carenze organizzative o mancati controlli. - Sanzioni AI Act: fino a € 35 M o 7 % del fatturato mondiale.	AI Act artt. 5 e 99; Legge 132/2025 artt. 14-16.
🟧 **Rischio alto** **(sistemi HR, credito, sanità, giustizia, infrastrutture)**	- Responsabilità disciplinare o professionale per uso negligente o senza supervisione. - Possibile responsabilità civile se la decisione automatizzata causa danno a terzi.	- Responsabilità oggettiva o concorrente per mancata valutazione di conformità, assenza di human-oversight o logging. - Obbligo di riparazione dei danni (AI Liability Directive in arrivo).	AI Act Titolo III (artt. 8-43); Legge 132/2025 artt. 7-12.
🟨 **Rischio limitato** **(chatbot, recommender, deepfake, IA conversazionale)**	- Responsabilità se omette di informare gli utenti o diffonde contenuti manipolatori o lesivi della reputazione. - Reato di diffusione di deepfake o manipolazioni dannose (art. 15 L. 132/2025).	- Obbligo di trasparenza e labeling dei contenuti AI. - Responsabilità civile per danno reputazionale o informativo.	AI Act art. 52; L. 132/2025 art. 15.
🟩 **Rischio minimo / nullo** **(filtri spam, traduttori, funzioni di supporto)**	- In genere nessuna responsabilità diretta, salvo dolo o colpa grave (es. uso improprio o fraudolento).	- Responsabilità solo se non adotta misure di sicurezza informatica o non previene abusi da parte di utenti.	AI Act art. 2 e Considerando 12.
⚙️ **Uso non controllato o inconsapevole** **(sistemi embedded o API integrate senza disclosure)**	- Responsabilità colposa per uso senza verifica o formazione adeguata. - Possibile violazione di obblighi deontologici (es. medico, avvocato, funzionario PA).	- Responsabilità per mancato controllo e assenza di governance AI. - In caso di danno, si valuta culpa in eligendo e in vigilando. - Rilevanza ai fini del D.Lgs. 231/2001.	AI Act art. 29-30; L. 132/2025 art. 11-12.
🏛️ **Pubblica Amministrazione**	- Il funzionario pubblico risponde civilmente e disciplinarmente se adotta decisioni basate su IA non autorizzata o senza trasparenza. - Possibile responsabilità erariale (Corte dei Conti).	- L'ente pubblico risponde per danno da provvedimento amministrativo viziato o per discriminazione algoritmica. - Obbligo di mappare e rendicontare l'uso di IA (art. 9 L. 132/2025).	Legge 132/2025 artt. 8-9 e 13.

tinexta cyber

Nuove fattispecie di reato in ambito AI

Normativa	Articolo / Codice	Data entrata in vigore	Descrizione
Legge 28 giugno 2024, n. 90 (“Cybersicurezza e reati informatici”)	• art. 615-ter c.p. • art. 615-quater c.p. • art. 629 c.p., comma 3 • art. 640 c.p., comma 2-ter • art. 24-bis D.Lgs. 231/2001	Entrata in vigore: 17 luglio 2024	Introduzione di: – inasprimento delle pene per l’accesso abusivo a sistemi informatici (art. 615-ter) e per la detenzione/divulgazione di strumenti di intercettazione informatica (art. 615-quater) – nuovo reato di “estorsione informatica” mediante accesso abusivo o minaccia connessa (art. 629 c.p., comma 3) – aumento pene per truffa commessa mediante strumenti informatici o telematici, art. 640 c.p. comma 2-ter – modifiche alla responsabilità degli enti (D.Lgs. 231/2001) in caso di reati informatici.
Legge n. 132/2025 (“Legge IA”) Legge 23 settembre 2025, n. 132	• art. 26 (Modifiche al Codice penale e ad ulteriori disposizioni penali) • nuovi art. (es. art. 612-quater c.p.) • art. 61 c.p., comma 11-decies (aggravante per uso IA) • art. 25 novies D.Lgs. 231/2001	Entrata in vigore: 10 ottobre 2025	Introduzione di: – un nuovo reato per la “diffusione illecita di contenuti generati o manipolati con sistemi di intelligenza artificiale” (art. 612-quater c.p.). – aggravante comune: l’uso di sistemi di intelligenza artificiale come modalità o mezzo del reato (art. 61 c.p., comma 11-decies) – impatti sulla responsabilità degli enti (modelli 231) con riferimento all’uso dell’IA come fattore di rischio
Norme endogene al D.Lgs. 231/2001 e responsabilità degli enti	Modifica dell’art. 24-bis D.Lgs. 231/01 per includere nuovi reati informatici o legati ai sistemi IA, con aumento delle sanzioni pecuniarie per gli enti	Entrata in vigore: 17 luglio 2024.	Riguarda la responsabilità di persone giuridiche per reati commessi tramite sistemi informatici/IA

Gli attori della normativa AI

ATTORE	DESCRIZIONE	ESEMPIO	OBBLIGHI	RESPONSABILITA'
Provider	Sviluppa e immette sul mercato il sistema AI	OpenAI, Siemens, IBM	Conformità, trasparenza, sicurezza, documentazione	Garantire che il sistema rispetti **tutti i requisiti dell'AI Act** (trasparenza, sicurezza, qualità dei dati, supervisione umana, ecc.). Redigere la **documentazione tecnica** e la **valutazione di conformità**. Mantenere una **"sintesi pubblica dei dati di training"** (per modelli GPAI). Apporre la **marcatura CE** per i sistemi ad alto rischio. Gestire **monitoraggio e correzioni** post-commercializzazione.
Deployer	Usa l'AI nei propri processi o servizi	Ospedale, banca, azienda	Uso corretto, supervisione umana, log e segnalazioni	Garantire che il sistema sia usato **in modo appropriato e conforme alla legge**. Mantenere **supervisione umana** nelle decisioni critiche. Informare le persone che interagiscono con un sistema AI (trasparenza). Tenere **tracciabilità e log** delle decisioni AI. In caso di sistemi ad alto rischio, **monitorare il funzionamento** e segnalare incidenti.
Distributor	Rivende o distribuisce un sistema AI sviluppato da altri	Marketplace software	Verifica conformità, nessuna modifica	Verificare che il sistema abbia la **marcatura CE** e la **documentazione conforme**. Non alterare le caratteristiche o la destinazione d'uso. Collaborare con le autorità in caso di richieste o ispezioni
User / End user	Interagisce col sistema ma non lo gestisce	Cliente o cittadino	Diritto all'informazione e ricorso	Nessuna responsabilità diretta

tinexta
cyber

Cosa dobbiamo fare?

Identificare e Governare l’AI nei Processi Aziendali: Azioni Concrete per un Uso Responsabile e Sicuro

tinexta
cyber

Percorso di adeguamento ad AI ACT e Legge 132/2025

1 AI ETHICAL ASSESSMENT

Obiettivo: mappare usi e impatti etici dell'IA in azienda o ente.
Attività chiave:
Individuare tutti i sistemi di IA in uso (interni, fornitori, embedded, sperimentali).
Valutare impatti su diritti fondamentali, equità, bias, trasparenza, controllo umano.
Classificare i sistemi secondo il livello di rischio (AI Act): inaccettabile, alto, limitato, minimo.
Identificare gap rispetto ai principi etici europei
Output: report di AI Ethical Impact Assessment (AEIA) → base per risk mapping

2 GAP ANALYSIS NORMATIVA

Obiettivo: verificare il livello di conformità legale e tecnica.
Attività chiave:
Analizzare i requisiti AI Act (Titolo III – high risk, GPAI, trasparenza).
Verificare aderenza alla Legge 132/2025 (obblighi su lavoro, sanità, ricerca).
Mappare sovrapposizioni con GDPR, cybersecurity e D.Lgs. 231/2001.
Valutare responsabilità contrattuali nella catena di fornitura AI.
Output: AI Compliance Matrix → elenco gap e priorità per ciascun sistema

3 GOVERNANCE E RUOLI

Obiettivo: istituire una struttura di governo dell'IA.
Attività chiave:
Nominare un AI Compliance Officer / AI Ethics Committee.
Definire ruoli: Provider, Deployer, Importer, User, secondo AI Act.
Allineare funzioni interne: Legal, DPO, IT Security, HR, R&D, Risk Management.
Adottare un AI Governance Framework (es. ISO/IEC 42001).
Output: AI Governance Charter – documento che definisce struttura, responsabilità e processi decisionali

4 POLICY E PROCEDURE

Obiettivo: tradurre i principi in regole operative.
Attività chiave:
Redigere o aggiornare policy aziendali:
-AI Use Policy (uso interno e terzi).
-AI Risk Management Procedure.
-Transparency & Human Oversight Policy.
-Incident & Post-Market Monitoring Procedure.
Integrare clausole di compliance AI nei contratti e nei bandi pubblici.
Output: pacchetto di policy aziendali integrate nella compliance 231/GDPR

5 IMPLEMENTAZIONE E FORMAZIONE

Obiettivo: mettere in atto i controlli e formare il personale.
Attività chiave:
Implementare strumenti di monitoraggio e logging AI.
Predisporre registri dei sistemi AI e documentazione tecnica (Annex IV AI Act).
Attivare percorsi di AI Literacy per lavoratori, manager e sviluppatori.
Sensibilizzare su rischi, bias e obblighi di trasparenza (art. 52 AI Act).
Output: personale formato + piattaforma di monitoraggio / registro AI interno

6 AUDIT, REVIEW E REPORTING

Obiettivo: garantire conformità continua e accountability.
Attività chiave:
Eseguire audit periodici (interni o di terze parti) sui sistemi AI.
Verificare performance, sicurezza, correttezza e assenza di discriminazioni.
Redigere AI Compliance Report annuale.
Coordinarsi con l'AI Office europeo e le autorità nazionali (Garante, AGID, Ministeri).
Output: dossier di conformità + readiness per eventuali ispezioni

tinexta
cyber

Flow chart e GANTT su 12 mesi

1) Ethical Assessment (mappatura usi, rischio, impatti etici)

2) Gap Analysis normativa (AI Act, L.132/2025, GDPR, 231)

3) Governance & Ruoli (AI Officer, RACI, comitato etico)

4) Policy & Procedure (trasparenza, oversight, incident)

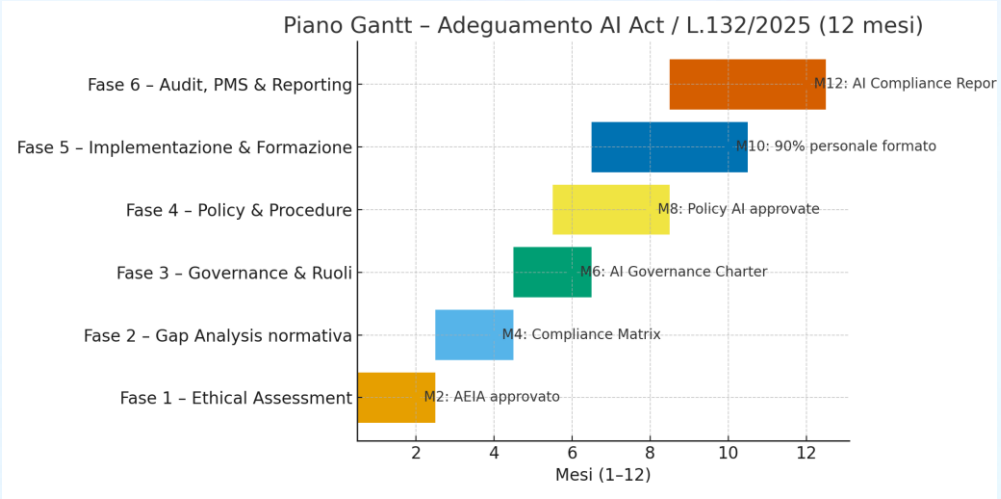
5) Implementazione & Formazione (logging, MRM, training)

6) Audit, PMS & Reporting (audit periodici, AI report)

FLUSSO DELLE ATTIVITA'

MILESTONES

M2: AEIA (AI Ethical Impact Assessment) approvato
M4: AI Compliance Matrix validata da Legal/DPO
M6: AI Governance Charter e RACI approvate dal Board
M8: Policy & Procedure AI pubblicate e operative
M10: 90% del personale formato (AI literacy)
M12: Audit concluso e AI Compliance Report rilasciato



tinexta cyber

Matrice RACI

Requisito / Attività	AI Officer	Legal / Compliance	DPO	IT / Data Gov	R&D / AI Eng.	Risk Mgmt / Audit	HR	Ethics Board	Top Mgmt
Mappatura e classificazione sistemi AI	R	C	C	R	C	I	I	C	**A**
AI Ethical Assessment iniziale	R	C	C	I	C	I	C	**A**	**A**
Gap analysis normativa (AI Act + L.132/2025)	C	R	C	I	I	C	I	I	**A**
Definizione AI Governance Framework	R	C	C	I	I	C	I	**A**	**A**
Redazione policy e procedure (uso AI, trasparenza, incident)	C	R	C	I	C	C	I	C	**A**
Valutazione e gestione del rischio (High-risk AI)	R	C	C	R	R	**A**	I	C	**A**
Logging, tracciabilità e audit trail	I	I	C	R	R	**A**	I	I	**A**
Supervisione umana e controlli etici	R	I	I	I	C	I	I	**A**	**A**
Trasparenza verso utenti e lavoratori (art. 52 AI Act / L.132/2025)	C	R	C	C	I	I	R	I	**A**
Formazione e AI literacy interna	I	C	I	I	I	C	R	I	**A**
Contratti e fornitura AI (supply chain)	C	R	C	I	I	C	I	I	**A**
Incident reporting / Post-market monitoring	R	C	C	R	R	**A**	I	C	**A**
Audit periodico e revisione annuale AI	C	C	C	C	C	R	I	C	**A**
Comunicazione pubblica e labeling contenuti AI	I	C	I	I	I	I	I	C	**A**
Relazione con autorità / AI Office / Garante	R	R	C	I	I	C	I	I	**A**

R = Responsible (esegue)
A = Accountable (decide e risponde)
C = Consulted (consulente/coinvolto)
I = Informed (informato)

tinexta cyber

Matrice RACI settore Privato

Attività / Requisito	AI Officer	Legal / Compliance	DPO	IT / Data Gov	R&D / AI Eng.	Risk / Audit	HR	Ethics Board	Top Mgmt
Mappatura e classificazione sistemi AI	R	C	C	R	C	I	I	C	A
AI Ethical Assessment iniziale	R	C	C	I	C	I	C	A	A
Gap analysis normativa	C	R	C	I	I	C	I	I	A
Definizione governance AI	R	C	C	I	I	C	I	A	A
Policy e procedure (uso, trasparenza, incident)	C	R	C	I	C	C	I	C	A
Gestione rischio (High-risk AI)	R	C	C	R	R	A	I	C	A
Logging e audit trail	I	I	C	R	R	A	I	I	A
Supervisione umana e controlli etici	R	I	I	I	C	I	I	A	A
Trasparenza verso utenti/lavoratori	C	R	C	C	I	I	R	I	A
Formazione e AI literacy	I	C	I	I	I	C	R	I	A
Contratti e fornitura AI	C	R	C	I	I	C	I	I	A
Incident reporting / Post-market monitoring	R	C	C	R	R	A	I	C	A
Audit e revisione annuale	C	C	C	C	C	R	I	C	A
Comunicazione e labeling contenuti AI	I	C	I	I	I	I	I	C	A

tinexta
cyber

Matrice RACI settore Pubblico

Nel settore pubblico le funzioni si adattano al contesto istituzionale: il Risk Management è spesso sostituito da Controllo Interno / RPCT (Responsabile della Prevenzione della Corruzione e della Trasparenza) e il Top Management coincide con la Direzione Generale o l'Organo politico.
Si aggiunge, inoltre, il **Responsabile della Transizione Digitale (RTD)**.

Attività / Requisito	AI Officer / RTD	Legal / Affari Generali	DPO	IT / Data Gov	Fornitore / Partner tecnico	Controllo Interno / RPCT	HR / Formazione	Comitato Etico	Direzione Generale
Mappatura sistemi AI in uso	R	C	C	R	C	I	I	C	A
Valutazione etica e impatto (AI Ethical Assessment)	R	C	C	I	C	I	C	A	A
Gap analysis normativa AI Act e L.132/2025	C	R	C	I	I	C	I	I	A
Definizione governance AI (delibera o circolare interna)	R	C	C	I	I	C	I	A	A
Policy e linee guida operative	C	R	C	I	C	C	I	C	A
Gestione rischio e trasparenza verso cittadini	R	C	C	R	R	A	I	C	A
Logging, audit e accountability	I	I	C	R	R	A	I	I	A
Supervisione umana decisioni automatizzate	R	I	I	I	C	I	I	A	A
Comunicazione pubblica e informazione cittadini	C	R	C	C	I	I	R	I	A
Formazione personale e dirigenti	I	C	I	I	I	C	R	I	A
Gestione contratti con fornitori AI	C	R	C	I	R	C	I	I	A
Incident reporting e notifiche Garante/AI Office	R	C	C	R	R	A	I	C	A
Audit periodico interno / esterno	C	C	C	C	C	R	I	C	A

tinexta
cyber

Cosa vuol dire utilizzo controllato e consapevole?

Impostare un modo d’uso intenzionale, trasparente e governato, in cui persone, processi e strumenti lavorano insieme per massimizzare valore e ridurre rischi (legali, operativi, etici, reputazionali).

tinexta
cyber

AI Literacy: alfabetizzazione all'intelligenza artificiale

Utilizzo consapevole dell'AI

Modello:

- Chiarezza di scopo: ogni caso d'uso ha un obiettivo di business dichiarato, KPI e metriche di successo/margine d'errore.
- Conoscenza dei limiti: si informano gli utenti sui limiti del sistema (allucinazioni, bias, privacy, copyright), quando NON usarlo e quando passare all'umano.
- Trasparenza: chi interagisce con contenuti o decisioni generate capisce che si tratta di out put IA (etichettatura/avvertenze).
- Formazione di ruolo: utenti, manager, sviluppatori e legali sanno cosa fare, cosa evitare e come segnalare anomalie.

Utilizzo controllato dell'AI

Modello:

- Policy e regole d'uso: linee guida chiare (dati ammessi/vietati, prompt sicuri, divieti, canali approvati).
- Ruoli e responsabilità: Owner del caso d'uso (business), Accountable (es. AI Officer), funzioni Consulted (Legal/DPO/IT), Informed (audit/board).
- Risk management: valutazioni prima del go-live (impatti su diritti, bias, IP, sicurezza), controlli di mitigazione e go/no-go documentato.
- Human-in-the-loop: supervisione umana nelle decisioni critiche; possibilità di override/appeal (contestare chiedendo intervento umano).
- Logging & auditability: tracciabilità dei dati in input/output, versioni dei modelli, prompt, parametri e decisioni.
- Sicurezza & privacy by design: classificazione dati, minimizzazione, cifratura, accessi minimi, segreti protetti, test di sicurezza (prompt-injection, data leakage).
- Monitoraggio continuo: alert su drift, qualità, tassi d'errore, incident reporting e correzioni.

tinexta cyber

Punti di attenzione

Componenti essenziali

- Use-case charter (scheda per caso d'uso): scopo, dati usati, basi giuridiche, metriche, rischi, owner, piani di fallback.
- Policy GenAI/AI: cosa è permesso, cosa no, strumenti approvati, gestione Intellectual Property e citazioni/copyright.
- Standard tecnici: MLOps/MRM (monitoraggio modelli), controlli di sicurezza (MFA, DLP, segregazione dati), ambienti separati (dev/test/prod).
- Processo di onboarding fornitori: due diligence, clausole di conformità, SLA su sicurezza, diritti d'autore, aggiornamenti modello.
- Formazione periodica: moduli base per tutti + avanzati per ruoli chiave (IT/Legal/Prodotto/HR).
- Meccanismo di segnalazione: canale rapido per bug, bias, violazioni (con presa in carico e feedback).
- Ciclo di vita documentato: dalla sperimentazione (sandbox/pilot) alla dismissione, con evidenze di test e approvazioni.

Esempi pratici

- Marketing: GenAI per draft di contenuti → policy su fonti e fact-checking; etichetta "contenuto generato con AI"; revisione umana obbligatoria.
- HR: screening CV assistito da AI → dataset validato, test di bias, spiegabilità delle raci, possibilità di revisione umana e canale di reclamo.
- Customer care: chatbot → disclosure "parli con un assistente AI", playbook di escalation a operatore, log conversazioni e filtro dati sensibili.
- Ricerca & sviluppo: uso di modelli generativi sul codice → repository separati, scansioni SAST/DAST, divieto di incollare segreti, licenze open-source verificate

Red Flags

- Upload di dati sensibili o segreti in strumenti non autorizzati.
- Decisioni senza controllo umano in ambiti critici (credito, lavoro, sanità).
- Mancanza di tracciabilità (impossibile ricostruire chi ha fatto cosa).
- Assenza di test di sicurezza (prompt injection, data exfiltration).
- Uso di modelli/fonitori senza clausole su copyright, privacy e sicurezza.

tinexta cyber

Esempi

Contesto	Esempio di uso controllato	Esempio di uso incontrollato	Rischio evitato / conseguenza
HR – screening CV	Modello valutativo validato, metriche di bias misurate, revisione umana obbligatoria, log delle decisioni.	Strumento generico che scarta CV "a scatola chiusa", senza tracciabilità né test di bias.	Discriminazione, contenziosi lavoro, sanzioni.
Marketing – copy generativi	Policy fonti, fact-checking umano, etichetta "contenuto creato con AI", archivio versioni.	Pubblicazione diretta di testi generati con info inesatte o IP non verificato.	Danno reputazionale, violazione copyright.
Customer care – chatbot	Disclosure "stai parlando con un'AI", regole di escalation a operatore, filtro PII, logging.	Bot senza filtri che chiede/archivia dati sensibili e fornisce istruzioni errate.	Data leak, reclami clienti, GDPR.
Finanza – antiriciclaggio	Modello con soglie motivate, explainability per alert, revisione investigativa, audit trimestrale.	Black-box che blocca transazioni senza motivazione né ricorso.	Danni a clienti, rischi regolatori.
R&D – coding assist	Repository dedicata, scanner SAST/DAST, divieto di incollare segreti, SBOM (elenco componenti Sw)	Copia/incolla di codice AI con licenze dubbie e chiavi API esposte.	Vulnerabilità, fuga segreti, violazioni licenza.
Sanità – triage clinico	Validazione clinica, supervisione medica, fallback manuale, registrazione decisioni.	Sistema di triage autonomo che decide priorità senza medico in loop.	Rischio paziente, responsabilità professionale.
Produzione – manutenzione predittiva	Sensori calibrati, soglie riviste dal plant manager, piano di intervento e rollback.	Modello che ferma la linea per falsi positivi, senza controllo umano.	Fermi impianto, costi e infortuni.
PA – servizi online	Modello che pre-classifica pratiche, operatore verifica e firma digitale la decisione.	Sistema che rifiuta domande automaticamente, senza motivazione né ricorso.	Vizi procedimentali, danno erariale.

Contesto	Esempio di uso consapevole	Esempio di uso inconsapevole	Rischio tipico
Vendite – e-mail	Il commerciale usa suggerimenti AI ma verifica numeri/offerte e personalizza.	Copia e invia testo AI con prezzi errati o promesse non autorizzate.	Contrattuale, reputazione.
Ufficio legale – ricerche	AI come "co-pilot" per bozze; citazioni verificate su banche dati ufficiali.	Affidarsi a citazioni "allucinate" senza controlli.	Errori legali, responsabilità.
Data analytics	GenAI per insight, poi controllo con query su dati di riferimento.	Decisioni prese su "pattern" inventati dal modello.	Decisioni sbagliate, costi.
Formazione interna	Corsi su limiti, bias, prompt sicuri; canale per segnalazioni.	Personale che incolla Informazioni personali o segreti in tool pubblici.	Data leak, GDPR/segseg.
Acquisti – vendor AI	Due diligence: sicurezza, IP, dati; clausole contrattuali AI (SLA, audit).	Adottare tool AI "freemium" senza valutare rischi o licenze.	Compliance, lock-in, IP.
Comunicazione	Etichetta dei contenuti sintetici e linee guida sui deepfake.	Pubblicazione di video AI senza disclosure, rischiando disinformazione.	Reputazione, norme settore.

tinexta cyber

Cosa fare

Segnali pratici per distinguere i quattro casi

- **Uso Controllato**: esistono policy, ruoli RACI, supervisione umana, log/audit, metriche di qualità e sicurezza.
- **Uso Incontrollato**: mancano regole, approvazioni, tracciabilità e test; decisioni automatizzate “al buio”.
- **Utilizzo Consapevole**: chi usa l’AI conosce scopi, limiti, dati ammessi, quando fermarsi e come chiedere aiuto.
- **Utilizzo Inconsapevole**: l’utente non sa che c’è AI o non ne capisce i limiti (bias, allucinazioni, privacy, Proprietà Intellettuale).

Le 5 domande da farsi

✓ **Scopo & KPI** sono chiari?
✓ C’è **supervisione umana** dove serve?
✓ Sono definiti **dati consentiti/vietati** (privacy/IP)?
✓ Esistono **log e audit trail** delle decisioni?
✓ **L’utente è stato formato** e sa come segnalare anomalie?

Output minimo consigliato

✓ **AI Use Policy** per tutta l’Azienda
✓ **Registro dei casi d’uso** con RACI e rischi
✓ **Procedure**: valutazione etica/legale, human-oversight, incident management
✓ **Formazione**: onboarding + refresh annual
✓ **Report trimestrale** su KPI qualità/rischi/incident

Perché serve un Codice Etico dell'AI?

E' necessario tradurre nella pratica i principi fondamentali europei

tinexta
cyber

Partire dal Codice Etico

Il Codice Etico serve a **collegare i principi astratti del diritto** (AI Act, GDPR, Carta dei Diritti UE) **alla realtà quotidiana** dell'azienda o dell'ente, ed è il cuore della governance responsabile dell'intelligenza artificiale
È ciò che **consente all'organizzazione di dimostrare "accountability" e affidabilità**, due pilastri centrali dell'AI Act e della Legge 132/2025.

Stabilisce regole comportamentali e decisionali coerenti con i sette principi etici dell'IA responsabile

1. **Human agency & oversight –** l'essere umano resta al centro del controllo decisionale
2. **Trasparenza –** l'IA deve essere comprensibile, spiegabile e dichiarata
3. **Affidabilità e sicurezza –** il sistema deve essere robusto, testato e gestito in sicurezza
4. **Privacy e governance dei dati –** rispetto dei diritti digitali e dei dati personali
5. **Equità e non discriminazione –** evitare bias e discriminazioni algoritmiche
6. **Accountability –** responsabilità chiara in ogni fase del ciclo di vita del sistema
7. **Sostenibilità e impatto sociale positivo –** uso etico e proporzionato alla finalità

A cosa serve

Ambito	Finalità pratica	Beneficio concreto
Governance	Fornire principi e linee guida a tutte le funzioni che usano o sviluppano IA.	Riduce rischio di comportamenti incoerenti o non conformi.
Decision making	Offrire criteri etici per decidere se adottare o meno una tecnologia AI.	Evita applicazioni rischiose o discriminatorie.
Compliance integrata	Allineare AI Act, Legge 132/2025, GDPR, D.Lgs. 231/2001, cybersecurity.	Migliora la difesa dell'organizzazione in caso di ispezioni o contenziosi.
Cultura e formazione	Diffondere consapevolezza e competenze sull'uso responsabile dell'IA.	Aumenta la fiducia interna ed esterna.
Reputazione e fiducia pubblica	Comunicare l'impegno etico verso clienti, dipendenti, cittadini.	Rafforza brand reputation e legittimazione sociale.

Il Codice Etico AI

- entra nel Modello 231/2001 come "codice di condotta AI";
- si collega alla politica di sicurezza informatica e al data governance framework;
- costituisce una mitigazione del rischio sanzionatorio in caso di violazioni o incidenti;
- è richiesto implicitamente dall'AI Act come parte della documentazione di conformità e accountability (artt. 9, 17, 29).

Perché è cruciale

Aspetto	Privato	Pubblico
Scopo principale	Dimostrare conformità e responsabilità sociale nell'uso di AI.	Garantire trasparenza, legalità e non discriminazione nei servizi pubblici.
Rischio mitigato	Reputazionale, legale e commerciale.	Giuridico, politico e amministrativo.
Effetto pratico	Aumenta fiducia di clienti, investitori e partner.	Rafforza fiducia dei cittadini e delle autorità di vigilanza.

tinexta cyber

Le procedure operative: il braccio tecnico del Codice Etico

Procedura	Obiettivo	Output atteso
AI Risk Management Procedure	Identificare e valutare rischi di bias, errori o impatti negativi.	Registro rischio AI e piano di mitigazione.
AI Transparency & Communication Procedure	Regolare modalità di informazione a utenti, clienti, dipendenti e cittadini.	Etichette, informative, disclaimer trasparenti.
AI Incident Reporting Procedure	Stabilire flussi per segnalazione anomalie o malfunzionamenti AI.	Registro incidenti e azioni correttive.
AI Procurement Procedure	Garantire che fornitori e partner rispettino AI Act e requisiti etici.	Clausole contrattuali standard AI compliance.
AI Training & Literacy Plan	Formare il personale sui rischi e sull'etica dell'IA.	Programma di formazione periodica.
AI Audit & Review Procedure	Monitorare l'efficacia delle policy e il rispetto del codice.	Audit report e aggiornamenti annuali.

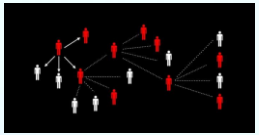
Esempio: procedura tecnico/organizzativo per tracciabilità

Nel contesto normativo europeo (AI ACT), **l' Articolo 19** ("Automatically generated logs") prevede che i fornitori di sistemi IA ad alto rischio conservino i log **per almeno sei mesi** (se ne hanno il controllo), salvo diversa disposizione del diritto dell'Unione o nazionale (nel contesto Italiano, Legge 132/2025).

- I sistemi di intelligenza artificiale **ad alto rischio** devono generare e conservare registri («log») delle operazioni, decisioni, anomalie, sorveglianza umana, input/output ecc
- Tali log devono essere **conservati** per un periodo pari **ad almeno sei mesi**, se il soggetto che utilizza o immette sul mercato il sistema ha il controllo di questi log

Obbligo teso ad assicurare **tracciabilità**, **responsabilità** e **auditabilità** dei sistemi IA ad alto rischio: in caso di incidenti, si deve poter risalire alla cronologia delle decisioni del sistema.

- Per **rispettare i requisiti di governance**, sorveglianza umana e monitoraggio previsti dal regolamento
- Per permettere alle autorità competenti di **effettuare ispezioni o valutazioni** del sistema anche più avanti nel tempo



LOG TIPICI

- *Input e output del sistema IA*
- *Informazioni su sorveglianza umana e override/appeal (se previsti)*
- *Eventuali anomalie, malfunzionamenti, errori o modifiche del modello (crash, bug, output errati, bias rilevati, modifiche al modello o ai suoi parametri)*
- *Eventi rilevanti per I diritti fondamentali, la sicurezza o la conformità del sistema (violazioni della privacy/discriminazioni, rischi per la sicurezza fisica/informatica, decisioni automatizzate che incidono su diritti umani)*

✅ **Cosa fare per essere conformi**

- ✓ Verificare se il sistema IA utilizzato è classificato come **ad alto rischio** (o comunque soggetto agli obblighi del regolamento)
- ✓ Implementare un sistema di logging che registri informazioni pertinenti e affidabili
- ✓ Garantire che i log siano archiviati per almeno sei mesi, e preferibilmente più a lungo se richiesto da normative nazionali o settoriali
- ✓ Definire procedure per conservazione sicura, accesso controllato, backup e integrità dei log

tinexta cyber


Formazione
Misura di sicurezza prodromica
tinexta
cyber

Il ruolo della formazione nel sistema di conformità AI

Formazione e awareness **non sono attività "accessorie",** ma il vero collante che **trasforma la norma in comportamento** concreto

AI Act (Reg. UE 2024/1689)

- **Art. 9, 29, 71**: impone formazione per garantire "appropriate human oversight" e "competenza del personale coinvolto".
- **Annex IV:** la documentazione tecnica deve dimostrare la qualificazione e la formazione del personale.
- **Art. 52**: trasparenza e consapevolezza degli utenti finali (devono sapere quando interagiscono con un'IA).

Legge italiana 132/2025

- **Art. 7–12**: richiede che operatori pubblici e privati siano formati sulla logica, parametri e metriche dei sistemi AI usati.
- **Art. 9 (PA):** obbligo per le amministrazioni di formare dipendenti e dirigenti sull'uso consapevole dell'IA.
- **Art. 15**: formazione obbligatoria sui rischi di deepfake e manipolazioni cognitive.

Funzione	Descrizione	Beneficio
Funzione preventiva	Riduce il rischio di errori umani, usi impropri, bias inconsapevoli o violazioni di trasparenza.	Diminuisce la probabilità di sanzioni o incidenti.
Funzione culturale	Diffonde una visione etica e consapevole dell'IA all'interno dell'organizzazione.	Crea fiducia interna e pubblica, rafforzando la reputazione.
Funzione dimostrativa	Serve a provare la "diligenza organizzativa" in caso di controlli o danni.	È una prova di compliance utile in sede di audit o giudizio.

Obiettivi strategici della formazione

Obiettivo	Descrizione pratica
Comprensione del rischio AI	Aiutare i dipendenti a riconoscere quando un sistema è ad alto rischio o richiede controlli speciali
Uso consapevole degli strumenti	Evitare uso improprio di chatbot, generatori, sistemi di raccomandazione o modelli interni
Riconoscimento dei bias	Saper individuare distorsioni nei dati o nei risultati algoritmici
Trasparenza e accountability	Comprendere obblighi di etichettatura, tracciabilità e logging
Segnalazione e incident reporting	Sapere come e quando segnalare un malfunzionamento AI o un impatto sui diritti

Target	Focus della formazione
Top management / Board	Risk governance, responsabilità, reputazione, reporting
AI Officer / Compliance / Legal	AI Act, Legge 132/2025, responsabilità e audit
IT, Data Science, R&D	Robustezza, sicurezza, tracciabilità, documentazione tecnica
HR e Comunicazione	Trasparenza, informazione dipendenti, bias nei processi
Tutti i dipendenti	Uso corretto di IA generativa, privacy, etichettatura, limiti legali

tinexta
cyber

Pianificazione

Voce	Settore Privato	Pubblica Amministrazione	Timeline 2025–2026	Milestone principali
Obiettivi formativi	• Conformità normativa (AI Act, GDPR, 231/2001) • Cultura etica e uso responsabile • Riduzione rischi legali e reputazionali • Formazione su accountability e logging	• Trasparenza e legalità dei processi automatizzati • Uso etico dell'IA nei servizi pubblici • Fiducia dei cittadini e accountability	Q1–Q2 2025: definizione obiettivi e piano formativo Q3–Q4 2025: prima erogazione corsi Q1–Q2 2026: aggiornamento e verifica risultati	• Approvazione del piano formativo AI • Inserimento nel piano di compliance aziendale o PIAO (Piano Integrato di Attività e Organizzazione per la PA) • Allineamento con AI Act in vigore
Destinatari	Top management, AI Officer, DPO, IT/Data Governance, HR, R&D, Compliance, Marketing	Dirigenti, RTD, DPO, funzionari, personale operativo, comunicazione istituzionale	Q2 2025: mappatura ruoli e fabbisogni formativi Q3 2025: coinvolgimento stakeholder	• Identificazione target formativi • Creazione elenco partecipanti e ruoli AI
Contenuti chiave	• AI Act: classificazione rischi e obblighi • Legge 132/2025 • Governance AI, bias e trasparenza • Incident management e audit • AI generativa e limiti d'uso	• AI Act e principi di trasparenza amministrativa • Legge 132/2025 art. 7–12 • Decisioni automatizzate e diritto di spiegazione • Etica pubblica e dati aperti	Q3–Q4 2025: sviluppo contenuti e validazione Q1 2026: aggiornamento moduli	• Sviluppo e approvazione contenuti • Validazione da AI Officer / RTD • Allineamento con linee guida AI Office UE
Modalità didattiche	• Workshop interattivi e e-learning • Casi pratici e simulazioni etiche • Ethical labs	• Formazione blended (aula + online) • Moduli PNRR competenze digitali • Webinar e simulazioni pubbliche	Q3–Q4 2025: erogazione iniziale Q1–Q2 2026: moduli avanzati e casi pratici	• Avvio piattaforma e-learning AI • Prime sessioni in aula • Valutazione partecipanti
Frequenza e durata	• Iniziale all'avvio + aggiornamento annuale • Refresh semestrale per ruoli critici	• Formazione annuale obbligatoria (art. 9 L.132/2025) • Aggiornamento su nuove linee guida AGID / AI Office	Continuo 2025–2026 con sessioni trimestrali e report annuale	• Aggiornamento piano annuale • Report di formazione e feedback
Indicatori di efficacia (KPI)	• % personale formato • Test di apprendimento >80% • Riduzione incidenti AI • Audit superati • Feedback positivi	• % personale formato • Segnalazioni etiche gestite • Audit interni/AGID positivi • Integrazione nel PIAO	Q2 2026: misurazione KPI e revisione piani	• Raccolta dati e KPI • Redazione AI Training Report • Audit di conformità
Output documentali	• Registro formazione AI • Attestati e materiali didattici • Piani annuali aggiornati • Report audit	• Registro formazione PA • Relazione RTD / RPCT • Integrazione nel Piano ICT / Anticorruzione	Q4 2025: prima raccolta evidenze Q2 2026: audit e rendicontazione	• Pubblicazione report formativo • Archiviazione evidenze per audit • Revisione documentazione AI Act

tinexta cyber

tinexta
cyber

Sfide nell’Implementazione dell’Intelligenza Artificiale

SFIDE

- ✓ **Competenze e risorse**: L’IA richiede conoscenze tecniche avanzate e infrastrutture adeguate.
- ✓ **Costi e manutenzione**: Integrazione, aggiornamento e gestione dei sistemi comportano investimenti e costi operativi continui.
- ✓ **Sicurezza e conformità**: È fondamentale garantire la protezione dei dati sensibili e il rispetto del GDPR.
- ✓ **Robustezza dei modelli**: I sistemi di IA devono essere resilienti a cyber attacchi e manipolazioni esterne.
- ✓ **Formazione del personale**: Occorre sviluppare competenze interne per un’adozione efficace dell’IA.
- ✓ **Trasformazione organizzativa**: L’adozione dell’IA implica spesso la revisione dei processi aziendali e del modello operativo.

AI come vantaggio competitivo

VANTAGGI

- ✓ **Costruire fiducia e qualità**, definendo policy di controllo dei modelli, monitorando le performance e comunicando in modo trasparente l'uso dell'IA;
- ✓ **Anticipare le normative,** integrando principi dell'AI Act nei processi;
- ✓ **Assecondare una innovazione sicura**, istituendo un comitato AI governance che valuti rischi, benefici e approvi i nuovi use case;
- ✓ **Rafforzare reputazione e brand,** predisponendo e pubblicando linee guida etiche, promuovendo casi d'uso sostenibili e comunicando l'impegno per un'IA responsabile;
- ✓ **Creare valore misurabile**, collegando i KPI dell'IA ai risultati di business (efficienza, qualità decisionale, riduzione errori).
- ✓ Integrare l'AI nel **binomio strategico Cybersecurity-ESG**

tinexta cyber

Q&A

Q&A e Contatti

✓**Domande durante il webinar:** utilizzare la chat messa a disposizione

✓**Contatti:** Sara Colnago *sara.colnago@tinextacyber.com*

✓**Link alla survey**:

https://www.tinextacyber.com/scopri-quanto-la-tua-azienda-e-pronta-a-gestire-lintelligenza-artificiale-in-modo-sicuro-e-responsabile/

tinexta cyber

PARTNER 24ORE NETWORK

Grazie!

tinexta cyber

think next,
secure now