ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI AVELLINO

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI SALERNO

CORSO PREPARATORIO AGLI ESAMI DI STATO

I sessione 2026

4 e 7 Settembre 2026

NORMATIVA TECNICA, VINCOLI, PROCEDURE E REGIMI AUTORIZZATORI

SETTORE INFORMAZIONE

Gestione dei Sistemi Informativi
Intelligenza Artificiale
Sicurezza delle Informazioni e Protezione dei Dati nell'era dell'AI Act

Relatore:
Ing. Roberto Santacroce - già Coordinatore della Commissione Trasformazione Digitale e Sicurezza delle Informazioni
Ing. Biagio Paruolo - già componente della Commissione Trasformazione Digitale e Sicurezza delle Informazioni

RUOLO E RESPONSABILITÀ DELL'INGEGNERE

Gestione dei Sistemi Informativi, Intelligenza Artificiale, Sicurezza delle Informazioni e Protezione dei Dati

nell'era dell'AI Act

La prospettiva del professionista: deontologia, privacy e conformità come parte del progetto

Ing. Biagio Paruolo – Ing. Roberto Santacroce

Agenda

1

Il ruolo e la responsabilità dell'ingegnere IT

Dalla competenza tecnica alla responsabilità giuridica

2

Deontologia applicata all'ambito IT

Codice deontologico, principi ed etica dell'IA

3

Privacy e protezione dei dati (GDPR)

Privacy by design: il progettista come attore della conformità

4

Intelligenza Artificiale e AI Act

Obblighi di chi progetta e utilizza sistemi di IA

PARTE 1 / 4

Il ruolo e la responsabilità dell'ingegnere IT

Dalla competenza tecnica all'assunzione di responsabilità

L'ingegnere dell'informazione: oltre il tecnico

- Il settore dell'informazione è una delle tre aree dell'Albo (con civile-ambientale e industriale)
- L'abilitazione non certifica il “saper fare” (già attestato dalla laurea) ma l'idoneità ad assumere responsabilità professionale
- L'iscrizione all'Albo comporta obblighi: competenza, deontologia, aggiornamento continuo, soggezione al potere disciplinare
- **L'ingegnere firma, progetta e garantisce: la sua firma è un'assunzione di responsabilità verso il committente e la collettività**

Sezioni A (laurea magistrale) e B (laurea triennale)

Le tre responsabilità del professionista

La stessa condotta può rilevare su piani diversi, anche insieme

1 Civile

Risarcimento del danno causato a committente o terzi (responsabilità contrattuale ed extracontrattuale).

2 Penale

Reati legati all'attività: dai delitti colposi ai reati informatici e sul trattamento dei dati.

3 Disciplinare

Violazione del codice deontologico: giudicata dal Consiglio di disciplina dell'Ordine.

Nell'IT il confine si allarga: un difetto di progetto software o una violazione di dati possono attivare tutti e tre i piani contemporaneamente.

L'ingegnere come garante di fiducia

Il rischio non è solo tecnico: è giuridico, economico e reputazionale

Qualità

Rispondere della bontà tecnica della soluzione, non solo del suo funzionamento immediato.

Sicurezza

Proteggere informazioni, sistemi e persone: la security è un requisito, non un'opzione.

Conformità

Garantire il rispetto delle regole (GDPR, AI Act, NIS2) sin dalla progettazione.

Etica

Considerare gli effetti su persone e società: ciò che è lecito non sempre è giusto.

PARTE 2 / 4

Deontologia applicata all'ambito IT

I doveri della professione, dalla riservatezza all'etica dell'IA

Deontologia e Codice Deontologico

- **Deontologia: l'insieme dei doveri e delle regole di condotta di una professione — ciò che si deve fare, oltre a ciò che è lecito**
- Il Codice Deontologico degli Ingegneri Italiani è emanato dal CNI e vincola tutti gli iscritti, in qualunque forma esercitino
- L'Ordine territoriale vigila; il Consiglio di disciplina giudica le violazioni e commina le sanzioni
- L'aggiornamento professionale è un obbligo deontologico (formazione continua e crediti formativi, dal DPR 137/2012)
- Etica ≠ legge: la deontologia può imporre di più e prima di quanto imponga la norma

Etica

Ciò che è giusto

Deontologia

I doveri della professione

Legge

Ciò che è obbligatorio

I principi deontologici fondamentali

1

Competenza e diligenza

Operare solo nell'ambito della propria competenza, con cura e preparazione adeguata.

2

Autonomia e indipendenza

Conservare autonomia di giudizio tecnico, libera da pressioni e conflitti d'interesse.

3

Correttezza e lealtà

Trasparenza verso il committente; concorrenza leale tra colleghi.

4

Riservatezza

Segreto professionale sulle informazioni acquisite nell'incarico.

5

Sicurezza e ambiente

Tutela dell'incolumità della collettività e sostenibilità ambientale.

6

Aggiornamento continuo

Mantenere e accrescere la competenza per tutta la vita professionale.

I principi calati nell'IT

Come ogni dovere deontologico prende forma concreta nel digitale

Riservatezza	Protezione dei dati e delle informazioni del committente → privacy e sicurezza (GDPR).
Competenza	Conoscere i limiti degli strumenti che si usano, IA compresa: non spacciare per infallibile un sistema che non lo è.
Autonomia	Non delegare all'algoritmo la decisione professionale; evitare il lock-in e i conflitti d'interesse coi fornitori.
Onestà intellettuale	Trasparenza sui limiti, sui rischi e sull'uso dell'IA; rispetto di licenze e proprietà intellettuale.

Dilemmi etici nel digitale e nell'IA

Bias e discriminazione

Algoritmi che ereditano pregiudizi dai dati e li applicano su larga scala.

Opacità decisionale

Sistemi “black-box”: chi risponde di una decisione che nessuno sa spiegare?

Automazione e responsabilità

Delegare all'IA rischia di diluire la responsabilità umana (“l'ha detto il sistema”).

Uso duale

Una stessa tecnologia può servire e nuocere: sorveglianza, deepfake, armi.

Privacy vs utilità

Più dati migliorano i modelli ma comprimono la riservatezza delle persone.

Sostenibilità

Il costo energetico e ambientale di addestramento e uso dei grandi modelli.

IA affidabile e IA nella professione

I principi europei dell'IA affidabile e le regole deontologiche recenti

IA affidabile — i 7 requisiti (UE)

- Sorveglianza e controllo umano
- Robustezza tecnica e sicurezza
- Riservatezza e governance dei dati
- Trasparenza e spiegabilità
- Diversità e non discriminazione
- Benessere sociale e ambientale
- Responsabilità (accountability)

IA e professione: le regole

- **L'IA può svolgere solo attività strumentali e di supporto**
- Il risultato deve restare frutto prevalente dell'attività intellettuale dell'ingegnere
- Obbligo di informare il cliente in modo chiaro sull'uso dell'IA
- La responsabilità resta in capo al professionista
- **Fonti: Codice Deontologico (integrato) e Legge 132/2025**

PARTE 3 / 4

3

Privacy e protezione dei dati (GDPR)

La conformità come requisito di progetto, non come adempimento

Il GDPR visto da chi progetta

- **Non un adempimento burocratico a valle, ma un insieme di requisiti che vincolano l'architettura del sistema**
- Minimizzazione → raccogliere solo i dati necessari: incide su schema dati, form, log
- Limitazione della finalità e della conservazione → politiche di retention e cancellazione by design
- Esattezza e integrità → validazione, versioning, sicurezza del dato
- Accountability → il titolare deve poter dimostrare la conformità: documentazione e scelte tecniche tracciate

Riferimenti

- GDPR — Reg. (UE) 2016/679
- Codice Privacy — D.Lgs. 196/2003 (novellato)
- Garante per la protezione dei dati personali
- Linee guida EDPB

I ruoli: dove si colloca l'ingegnere

Titolare

Decide finalità e mezzi del trattamento. È il cliente/l'organizzazione.

Responsabile

Tratta i dati per conto del titolare: qui rientra spesso il fornitore IT.

Sub-responsabile

Fornitori a valle (es. cloud provider): vanno vincolati contrattualmente.

DPO

Sorveglia e consiglia; obbligatorio in alcuni casi.

Il punto per l'ingegnere: chi sviluppa o gestisce sistemi è di norma responsabile del trattamento (art. 28), legato al titolare da un contratto che impone misure e istruzioni. Non è titolare, ma le sue scelte tecniche determinano la conformità.

Privacy by design & by default (art. 25)

Il cuore del GDPR per il progettista: la protezione si costruisce, non si aggiunge

Il principio

- By design: protezione dei dati integrata fin dalla progettazione del sistema
- By default: l'impostazione predefinita è quella più protettiva per l'utente
- Vale per l'intero ciclo di vita: raccolta, uso, conservazione, cancellazione

Le tecniche

- Minimizzazione dei dati raccolti
- Pseudonimizzazione e anonimizzazione
- Cifratura a riposo e in transito
- Controllo degli accessi e profili minimi
- Retention e cancellazione automatiche
- Default privacy-friendly (opt-in, non opt-out)

Sicurezza, DPIA e violazioni dei dati

Sicurezza del trattamento

Art. 32 — misure tecniche e organizzative adeguate al rischio: cifratura, resilienza, test periodici.

Valutazione d'impatto (DPIA)

Art. 35 — obbligatoria per trattamenti ad alto rischio (nuove tecnologie, larga scala, profilazione).

Data breach

Art. 33-34 — notifica al Garante entro 72 ore; comunicazione agli interessati se alto rischio.

Sicurezza ↔ privacy

La security (art. 32) è il mezzo tecnico della protezione dei dati: qui i due temi coincidono.

Diritti, decisioni automatizzate e sanzioni

- Diritti dell'interessato: accesso, rettifica, cancellazione (oblio), limitazione, opposizione, portabilità
- **Art. 22 — diritto a non essere sottoposti a decisioni unicamente automatizzate con effetti significativi**
- → richiede intervento umano, informazione e possibilità di contestare: crocevia con l'IA
- Trasferimenti extra-UE: garanzie adeguate (clausole tipo, decisioni di adeguatezza)
- Sanzioni: fino a 20 milioni di euro o il 4% del fatturato mondiale annuo

Sanzione massima

20 M€

oppure 4% del fatturato mondiale

GDPR: storia e obiettivo

Dal diritto alla protezione dei dati alla conformità progettata

Perché nasce

Per armonizzare le regole europee e rafforzare i diritti delle persone in un mercato digitale unico.

Cosa cambia

Da “adempimento” a responsabilità dimostrabile: il titolare deve provare scelte, misure e controlli.

Acronimo

GDPR = General Data Protection Regulation, cioè Regolamento generale sulla protezione dei dati.

1995
Direttiva 95/46/CE

2016
Reg. (UE) 2016/679

2018
Applicazione dal 25 maggio

Oggi
cloud, IA, dati globali

Idea chiave: il dato personale non è “materia prima libera”, ma un diritto fondamentale da trattare con limiti, trasparenza e sicurezza.

Rif.: GDPR Reg. (UE) 2016/679, considerando 1, artt. 5, 24-25.

I punti salienti del GDPR

Gli otto concetti da ricordare e tradurre in requisiti tecnici

1 Liceità, correttezza, trasparenza
Base giuridica chiara e informativa comprensibile.

2 Finalità
Uso dei dati limitato allo scopo dichiarato.

3 Minimizzazione
Solo i dati necessari, niente raccolta “per sicurezza”.

4 Esattezza
Dati aggiornati, validati e correggibili.

5 Conservazione
Retention definita; cancellazione o anonimizzazione.

6 Integrità e riservatezza
Sicurezza, cifratura, accessi controllati.

7 Accountability
Dimostrare la conformità con evidenze e log.

8 Diritti
Accesso, rettifica, oblio, portabilità, opposizione.

Per il progettista: questi principi diventano scelte su database, form, log, permessi, backup, retention e contratti.

Rif.: GDPR art. 5 e diritti degli interessati artt. 12-22.

Dati personali, ruoli e basi giuridiche

Prima di progettare bisogna sapere cosa si tratta, perché e per conto di chi

Dato personale

Qualsiasi informazione che identifica o rende identificabile una persona: nome, email, IP, log, posizione, identificativi online.

Categorie particolari

Dati più delicati: salute, biometria, opinioni, origine, convinzioni. Richiedono garanzie rafforzate.

Base giuridica

Consenso, contratto, obbligo legale, interesse pubblico, interesse legittimo o tutela di interessi vitali.

Titolare

decide finalità e mezzi

Responsabile

tratta su istruzioni

DPO

consiglia e sorveglia

Acronimi: DPO = Data Protection Officer / Responsabile della protezione dei dati; IP = Internet Protocol.

DPIA: valutazione d’impatto

Proteggere prima: quando il trattamento può generare rischio elevato

1 Quando

nuove tecnologie, larga scala, profilazione, dati sensibili

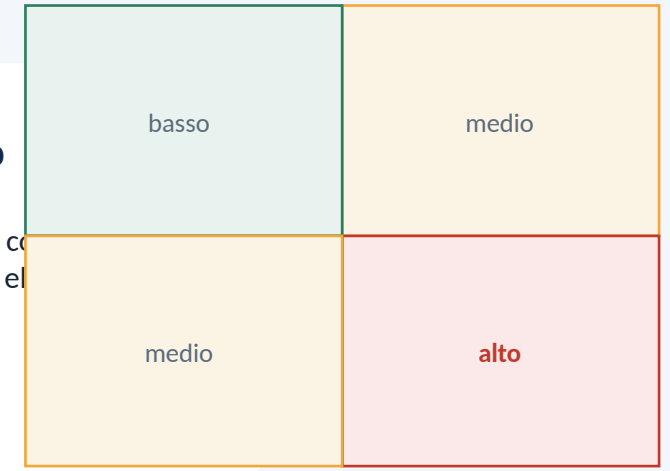
2 Cosa

descrivere trattamento, rischi, necessità, proporzionalità, misure

3 Esito

ridurre il rischio; c
Garante se resta el

Rischio = probabilità × impatto



Acronimo DPIA = Data Protection Impact Assessment: valutazione preventiva, non documento compilato a posteriori.

Rif.: GDPR art. 35-36; linee guida EDPB sulla DPIA.

Cloud: responsabilità condivisa

Il cloud non elimina gli obblighi: li distribuisce fra contratti, configurazioni e controlli

Titolare / cliente

Definisce finalità, dati, base giuridica, retention e istruzioni al fornitore.

Responsabile IT

Esegue istruzioni, applica misure, gestisce sub-fornitori e prove di sicurezza.

Cloud provider

Infrastruttura, servizi, region, certificazioni, logging, cifratura e continuità.

Da verificare nel progetto

DPA art. 28 · sub-responsabili · region/data residency · trasferimenti extra-UE · cifratura · log · SLA · diritto di audit

Acronimi: DPA = Data Processing Agreement; SCC = clausole contrattuali tipo; SLA = livelli di servizio; IAM = gestione identità e accessi.

IA e protezione dei dati

Con l'intelligenza artificiale il dato può entrare in training, prompt, output e log

Addestramento

dataset e fine-tuning

Prompt

input dell'utente

Output

risposte e decisioni

Log

tracciamento e audit

Rischi privacy

- riuso dei dati per addestrare modelli
- inferenza di dati sensibili
- bias e profilazione
- decisioni automatizzate senza controllo umano

Misure di controllo

- minimizzazione e pseudonimizzazione
- base giuridica e informativa
- retention dei log
- human-in-the-loop e audit

Nota: IA = Intelligenza Artificiale; human-in-the-loop = intervento umano nel processo decisionale.

Business Continuity e Disaster Recovery

La disponibilità del dato è parte della protezione: senza servizio, anche i diritti si fermano

BCP

Business Continuity Plan: come mantenere operativi processi e servizi essenziali durante un incidente.

DRP

Disaster Recovery Plan: come ripristinare sistemi, dati e infrastruttura dopo un evento grave.

BIA

Business Impact Analysis: stima impatti, priorità e dipendenze dei processi critici.

RTO

Recovery Time Objective: tempo massimo accettabile di fermo.

RPO

Recovery Point Objective: quantità massima di dati perdibili.

Checklist: backup 3-2-1, test di restore, runbook, ruoli, fornitori, comunicazione, riesame periodico.

Data breach: esempio e 72 ore

Violazione di sicurezza: perdita, modifica, divulgazione o accesso non autorizzato

Esempio

Ransomware su server di uno studio: esfiltrati documenti, contratti, copie documento e dati dei clienti. Il backup c'è, ma va verificata la copia fuori perimetro.

T0

Rileva

isola sistemi, conserva evidenze

+24h

Valuta

dati, soggetti, rischio, impatto

entro

Notifica

al Garante se rischio probabile

se alto

Comunica

agli interessati con istruzioni

Il responsabile del trattamento informa tempestivamente il titolare; le notifiche oltre 72 ore devono motivare il ritardo.

Rif.: GDPR artt. 33-34; indicazioni del Garante data breach.

Garante e sanzioni

L'Autorità di controllo non è solo "multa": può verificare, ordinare e limitare trattamenti

Garante privacy

Autorità italiana per la protezione dei dati personali: riceve reclami e breach, svolge controlli, emette provvedimenti.

Poteri

Ammonire, ordinare adeguamenti, limitare o vietare trattamenti, imporre la cancellazione dei dati.

Sanzioni massime

10 M€ / 2%
violazioni meno gravi

20 M€ / 4%
violazioni più gravi

La sanzione dipende da gravità, durata, dolo/colpa, misure adottate, cooperazione, precedenti e categorie di dati.

Rif.: GDPR art. 83; poteri Autorità artt. 57-58.

Sicurezza dei dati: checklist di progetto

Misure tecniche e organizzative adeguate al rischio: non solo tecnologia, anche processi

Governance	registro, ruoli, policy, formazione
Identità	IAM, MFA, profili minimi, segregazione
Dati	cifratura, pseudonimizzazione, retention, DLP
App & Cloud	hardening, patching, logging, secret management
Monitoraggio	SIEM, EDR, incident response, test periodici

Acronimi: MFA = autenticazione a più fattori; SIEM = raccolta/correlazione eventi; DLP = prevenzione perdita dati; EDR = rilevamento e risposta sugli endpoint.

Rif.: GDPR art. 32 sicurezza del trattamento.

Figure GDPR: responsabilità operative

Chi decide, chi esegue, chi controlla: ruoli da chiarire nel progetto

Diritti

Interessato

Persona fisica cui si riferiscono i dati. Ha diritti esercitabili: accesso, rettifica, cancellazione, limitazione, opposizione e portabilità.

Decide

Titolare del trattamento

Decide finalità e mezzi: perché trattare, quali dati, base giuridica, informativa, retention e governance complessiva.

Esegue

Responsabile del trattamento

Tratta dati per conto del titolare con istruzioni documentate; deve garantire misure adeguate e cooperare in audit e breach.

Supporta

Sub-responsabile

Fornitore a valle del responsabile, spesso cloud/SaaS. Serve autorizzazione e contratto con obblighi equivalenti.

Sorveglia

DPO

Data Protection Officer: indipendente; informa, consiglia, sorveglia la conformità, esprime pareri su DPIA e dialoga con il Garante.

Opera

Amministratore di sistema

Ruolo tecnico con privilegi elevati: nomina/autorizzazione, istruzioni, log, segregazione dei compiti e verifiche periodiche.

Punto chiave: il contratto art. 28, le istruzioni documentate e la matrice dei ruoli vanno definiti prima di sviluppare o configurare il sistema.

Acronimi: GDPR = General Data Protection Regulation; DPO = Data Protection Officer; SaaS = Software as a Service.

DPIA: quando farla e cosa deve produrre

La valutazione d'impatto è un processo di progetto, non un allegato finale

Quando è richiesta

- Nuove tecnologie con rischio elevato
- Profilazione o decisioni automatizzate rilevanti
- Monitoraggio sistematico di aree/accessi/utenti
- Trattamenti su larga scala o dati particolari
- Incrocio di banche dati o sorveglianza continua

Contenuto minimo

- Descrizione del trattamento e finalità
- Categorie di dati, interessati e flussi
- Sistemi, fornitori, trasferimenti e retention
- Necessità e proporzionalità
- Rischi per diritti e libertà delle persone
- Misure tecniche e organizzative di mitigazione

Output operativo

- Decisioni motivate e tracciabili
- Rischio residuo accettato o ridotto
- Piano di remediation con owner e scadenze
- Parere DPO quando presente
- Consultazione preventiva del Garante se il rischio resta elevato

Acronimi: DPIA = Data Protection Impact Assessment; DPO = Data Protection Officer.

Politica di backup 3-2-1

Dal principio alla prova di recupero: continuità, resilienza e responsabilità

3 **copie**

1 dato originale + 2 copie di backup

2 **supporti**

copie su tecnologie o storage differenti

1 **off-site**

una copia separata, preferibilmente offline o immutabile

Controlli tecnici

- Cifratura dei backup e gestione sicura delle chiavi
- Versioning e retention coerenti con i tempi GDPR
- Protezione ransomware: copie immutabili/offline
- Monitoraggio esiti, alert e log delle operazioni

Controlli organizzativi

- Test periodici di restore, non solo verifica “backup ok”
- Runbook: chi fa cosa, tempi, escalation e contatti
- RTO e RPO dichiarati, misurati e riesaminati
- Esercitazioni su scenari: guasto, errore umano, attacco

RTO Recovery Time Objective: tempo massimo accettabile di fermo.

RPO Recovery Point Objective: quantità massima di dati che si può perdere.

Acronimi: RTO = Recovery Time Objective; RPO = Recovery Point Objective; DR = Disaster Recovery.

Infografica GDPR: ruoli, rischio, continuità

La conformità si costruisce con responsabilità chiare, DPIA e recuperabilità dei dati

1 Ruoli chiari

Titolare	decide finalità e mezzi
Resp.	esegue su istruzioni
DPO	sorveglia e consiglia

Contratti, istruzioni e autorizzazioni rendono verificabile la catena delle responsabilità.

2 DPIA

Mappa	dati, flussi, fornitori
Valuta	probabilità × impatto
Mitiga	misure e rischio residuo

La DPIA documenta le decisioni prima che il rischio ricada sulle persone.

3 Backup 3-2-1

Copie	originale + due backup
Supporti	tecnologie differenti
Off-site	separata/immutabile

Il backup è misura di sicurezza solo se il ripristino è provato.

Messaggio chiave: GDPR = progettazione verificabile di ruoli, rischi, misure e continuità operativa.

Acronimi: DPIA = Data Protection Impact Assessment; GDPR = Regolamento generale sulla protezione dei dati.

Parte 3 — da ricordare all'orale

Non è burocrazia

Il GDPR vincola l'architettura: minimizzazione, retention, sicurezza si progettano dentro il sistema.

Ruolo

L'ingegnere/fornitore è di norma responsabile del trattamento (art. 28); le sue scelte fanno la conformità.

Art. 25

Privacy by design & by default: cifratura, pseudonimizzazione, default protettivi, minimizzazione.

Adempimenti

Art. 32 sicurezza e backup 3-2-1, art. 35 DPIA, breach 72h, art. 22 decisioni automatizzate. Sanzioni 20M€/4%.

PARTE 4 / 4

Intelligenza Artificiale e AI Act

Gli obblighi di chi progetta e utilizza sistemi di IA

4

AI Act in pillole: dove lavora l'ingegnere

Reg. (UE) 2024/1689 — approccio basato sul rischio; il grosso degli obblighi è sull'alto rischio

Inaccettabile	Vietato
Alto rischio	**Requisiti stringenti — è qui che si concentra il lavoro dell'ingegnere**
Limitato	Obblighi di trasparenza (art. 50)
Minimo	Libero

Sistemi ad alto rischio: i requisiti

Cosa deve garantire chi progetta un sistema di IA ad alto rischio

1

Gestione del rischio

Processo iterativo lungo tutto il ciclo di vita (art. 9).

2

Governance dei dati

Dataset pertinenti, rappresentativi, corretti; controllo dei bias (art. 10).

3

Documentazione e log

Documentazione tecnica e registrazione automatica degli eventi (art. 11-12).

4

Trasparenza

Istruzioni chiare per l'utilizzatore; comprensibilità dell'output (art. 13).

5

Sorveglianza umana

Il sistema deve poter essere supervisionato e fermato da una persona (art. 14).

6

Accuratezza e robustezza

Prestazioni, resilienza e cybersicurezza adeguate (art. 15).

Chi risponde: fornitore e utilizzatore

Fornitore (provider)

Sviluppa o fa sviluppare il sistema e lo immette sul mercato a proprio nome.

Sopporta gli obblighi principali: requisiti, valutazione di conformità, marcatura CE, documentazione.

Utilizzatore (deployer)

Impiega il sistema nell'ambito della propria attività professionale.

Obblighi propri: uso conforme alle istruzioni, sorveglianza umana, monitoraggio, informazione.

Dove sta l'ingegnere? Può trovarsi in ambedue le posizioni, ma attenzione: modificare sostanzialmente un sistema può far diventare fornitori.

Conformità, marcatura CE e scadenze

- **I sistemi ad alto rischio seguono una valutazione di conformità prima dell'immissione sul mercato**
- Esito: marcatura CE, dichiarazione di conformità e registrazione nella banca dati UE
- Sistema di gestione della qualità e sorveglianza post-commercializzazione
- Trasparenza (art. 50): dichiarare l'interazione con l'IA, i deepfake e i contenuti generati
- **Logica analoga alla marcatura CE dei prodotti: territorio familiare per l'ingegnere**

feb 2025
Divieti

ago 2025
Modelli GPAI, governance

ago 2026
Piena applicazione — alto rischio + art. 50

ago 2027
Alto rischio nei prodotti CE

★ 2 agosto 2026: la data chiave

La doppia conformità del progettista

Un sistema di IA che tratta dati personali risponde a GDPR e AI Act insieme

Base e finalità	GDPR: base giuridica, minimizzazione, finalità del trattamento (anche per l'addestramento).
Trasparenza	GDPR (informativa) + AI Act art. 50: convergono nell'obbligo di dire che c'è un'IA.
Sorveglianza umana	Art. 22 GDPR + art. 14 AI Act: la decisione automatizzata richiede controllo umano.
Valutazioni	DPIA (GDPR) e gestione del rischio (AI Act): stessa logica, da coordinare in un unico processo.

La Legge 132/2025 in sintesi

In vigore dal 10 ottobre 2025 — approccio antropocentrico, coordinato con l'AI Act (Reg. UE 2024/1689)

Struttura	6 Capi e 28 articoli; numerosi aspetti sono rimessi a decreti attuativi ancora da adottare.
Capo I	Finalità e principi generali dell'uso dell'intelligenza artificiale.
Capo II	Disposizioni settoriali: sanità, lavoro, professioni, pubblica amministrazione, giustizia.
Capi III–VI	Governance, diritto d'autore, profili penali e disposizioni finali.

La 132/2025 per l'ingegnere (1/2)

Principi generali, dati e professione intellettuale

Art. 3 — Principi generali	Diritti fondamentali, trasparenza, sicurezza, autonomia umana, prevenzione del danno, non discriminazione, sostenibilità, cybersicurezza, accessibilità.
Art. 4 e 9 — Dati e informazione	Trattamento conforme al GDPR; informazioni rese con linguaggio chiaro, semplice e comprensibile.
Artt. 11-12 — Lavoro	Informare i lavoratori sui sistemi decisionali automatizzati; tutela contro la discriminazione automatizzata.
Art. 13 — Professioni intellettuali	IA solo strumentale e di supporto, con prevalenza del lavoro intellettuale; responsabilità del professionista e informativa chiara al cliente.

La 132/2025 per l'ingegnere (2/2)

Opere, responsabilità penale e ambiti settoriali

Art. 25 — Diritto d'autore	Tutela estesa alle opere create con l'ausilio dell'IA; disciplina dell'estrazione di testi e dati (text and data mining).
Art. 26 — Profili penali	Nuovo art. 612-quater c.p. contro la diffusione illecita di contenuti generati o manipolati con IA (deepfake).
Ambiti settoriali	Sanità (artt. 7-10), P.A. (art. 14), giustizia (art. 15): supervisione umana rafforzata sulle decisioni che incidono su diritti.

Prima di adottare l'IA: le attività preliminari

Cosa mettere in campo prima di introdurre un sistema di IA in un ambito

Analisi del rischio	Individuare ambito, finalità e livello di rischio; valutare gli impatti su persone, dati e sicurezza prima di partire.
Formazione dei dipendenti	Preparare chi userà l'IA: competenze di base, limiti, uso responsabile e obblighi informativi.
Capacità di monitoraggio	Predisporre log, indicatori di qualità e sorveglianza umana per controllare gli output nel tempo.
Controlli periodici	Audit, riesami e aggiornamenti programmati per mantenere nel tempo conformità e sicurezza.

Analisi del rischio e formazione

Analisi del rischio

Definire ambito e finalità dell'IA; classificare il livello di rischio, anche secondo l'AI Act.

Valutare impatti su persone, dati e sicurezza; DPIA se si trattano dati personali; documentare le scelte.

Formazione dei dipendenti

Competenze di base sull'IA, sui suoi limiti e sui rischi: bias, errori, output inaffidabili.

Uso corretto e responsabile, obblighi informativi, chiara attribuzione di ruoli e responsabilità.

Il punto: capire il rischio prima di agire, e mettere le persone in condizione di usare l'IA con consapevolezza.

Monitoraggio e controlli periodici

Capacità di monitoraggio

Log e tracciabilità; indicatori di qualità e prestazione dell'output; rilevazione di anomalie e drift.

Sorveglianza umana effettiva (human-in-the-loop) e canali chiari per segnalare i malfunzionamenti.

Controlli periodici

Audit e riesami programmati; verifica continua di conformità a GDPR e AI Act.

Aggiornamento di sistema e dataset, gestione degli incidenti, revisione della documentazione.

Il punto: adottare l'IA non è un atto una tantum: va sorvegliata e ricontrollata lungo tutto il ciclo di vita.

Analisi del rischio: come si fa

Prima di introdurre l'IA occorre capire cosa può andare storto e chi ne subirebbe le conseguenze: si procede per passi.

Come si fa, passo per passo

1. Definire il contesto: quale attività, con quale finalità e con quali dati.
2. Individuare i rischi: errori dell'output, bias, uso improprio, dati e sicurezza.
3. Stimare probabilità e gravità di ciascun rischio (matrice del rischio).
4. Definire le mitigazioni: supervisione umana, soglie di allerta, verifiche.
5. Documentare, classificare (anche per l'AI Act) e rivalutare quando qualcosa cambia.

Esempio pratico

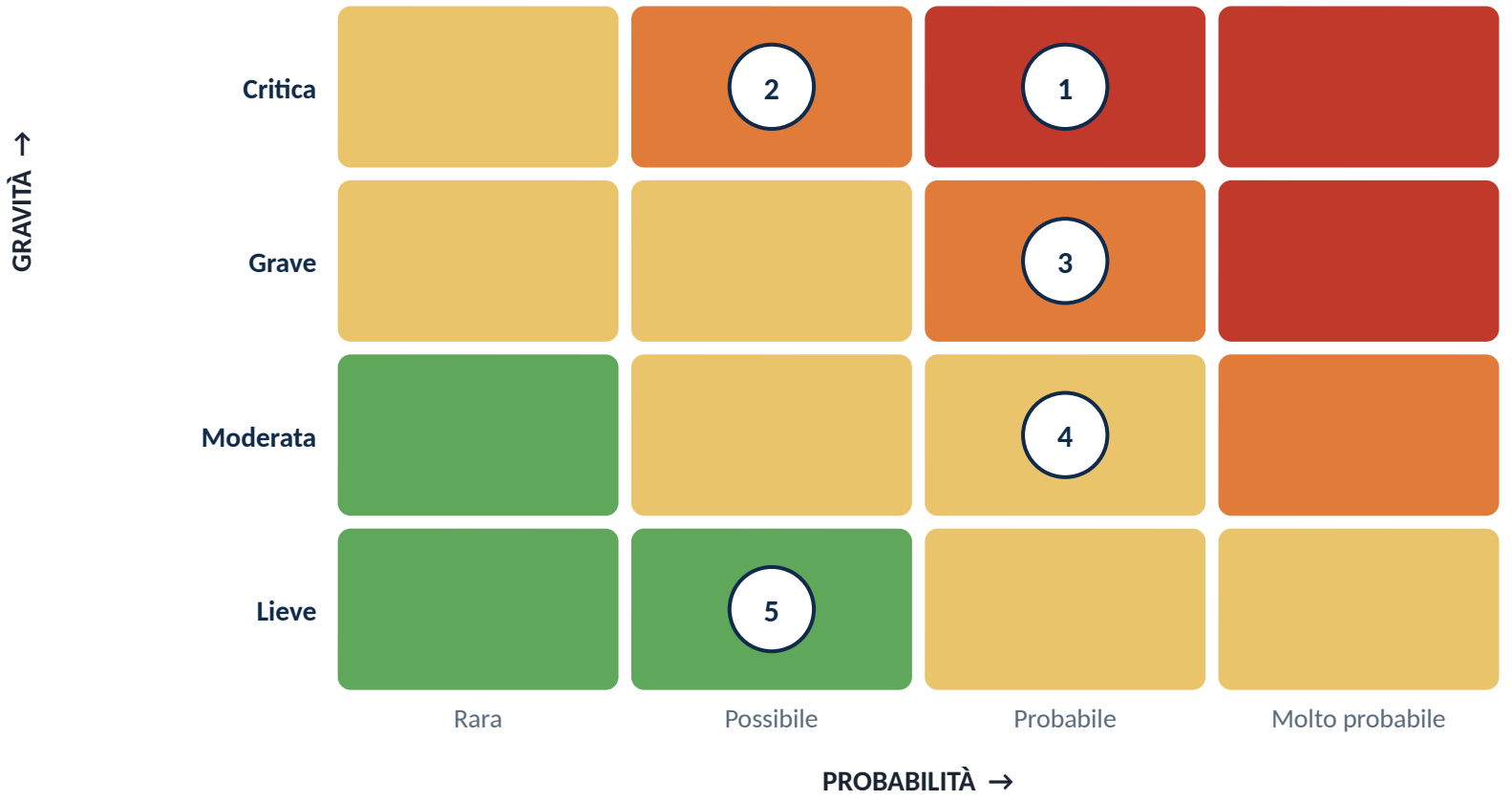
Uno studio adotta un'IA che segnala anomalie nelle verifiche strutturali. Il rischio critico è il falso negativo: un problema reale non viene rilevato.

Gravità alta, probabilità media. Mitigazione: l'ingegnere valida sempre gli esiti critici, fissa soglie prudenziali e registra i casi dubbi.

In sintesi: il rischio si governa prima di adottare l'IA, non dopo il primo errore.

Analisi del rischio dell'IA: la matrice

Probabilità × gravità: dove si colloca ogni rischio e come orientare le priorità di trattamento



I rischi individuati

1 Falso negativo strutturale **(Estremo)**

2 Violazione dati personali **(Alto)**

3 Bias discriminatorio **(Alto)**

4 Drift del modello nel tempo **(Medio)**

5 Allucinazione minore **(Basso)**

Livello di rischio

Basso | Medio | Alto | Estremo

Audit periodici: come si fanno

L'audit periodico verifica che il sistema funzioni ancora bene e resti conforme nel tempo: è un controllo pianificato e documentato.

Come si fa, passo per passo

1. Pianificare cadenza e ambito (es. ogni 6-12 mesi o dopo modifiche rilevanti).
2. Raccogliere le evidenze: log, metriche di qualità, segnalazioni, incidenti.
3. Verificare la conformità a GDPR, AI Act e procedure interne.
4. Testare le prestazioni: risultati attesi contro reali, bias e «drift».
5. Registrare rilievi e azioni correttive, con responsabili e scadenze.

Esempio pratico

A 12 mesi l'accuratezza dell'IA è calata: i dati reali sono cambiati rispetto a quelli di addestramento (fenomeno di «drift»).

Azione correttiva: ri-addestramento con dati aggiornati, nuova validazione, aggiornamento della documentazione e verifica di controllo dopo 3 mesi.

In sintesi: adottare l'IA non è un atto una tantum: si verifica e si corregge lungo tutto il ciclo di vita.

Il filo conduttore

Un unico principio attraversa tutto: la responsabilità si progetta

Ruolo
L'ingegnere risponde

→

Deontologia
...secondo i suoi doveri

→

Privacy
...tutelando le persone

→

AI Act
...e governando l'IA

"by design" — qualità, sicurezza, privacy e conformità non si aggiungono a fine progetto: si costruiscono dentro, dalla prima riga. È questo che distingue l'ingegnere dal tecnico.

Grazie

Domande e discussione

Ruolo dell'ingegnere · Deontologia · Privacy e GDPR · AI Act