

## Legge 132/2025 - Regolamento (UE) 2024/1689 (AI Act)

**Sintesi generata con il supporto di Gemini convalidata e condivisa dal Docente**

### I - Pilastri della Norma

#### 1. Governance e Vigilanza (Chi controlla?)

La Legge 132/2025 designa le autorità nazionali competenti per l'applicazione dell'AI Act :

- **AgID** (Agenzia per l'Italia Digitale): Si occupa della promozione dell'innovazione e della verifica della conformità tecnica. È l'interlocutore principale per la PA.
  - **ACN** (Agenzia per la Cybersicurezza Nazionale): Vigilanza sugli aspetti di sicurezza informatica dei sistemi di IA.
  - **Garante Privacy**: Resta l'autorità suprema per quanto riguarda l'impatto dei sistemi di IA sui dati personali e sulla profilazione.
- 

#### 2. L'IA nel Lavoro Pubblico (Art. 10 e segg.)

- **Obbligo di Formazione**: La legge impone alle PA di formare il personale sull'uso etico e critico dell'IA. (La tua docenza di domani assolve proprio a questo precetto legislativo!).
  - **Trasparenza verso il Lavoratore**: Se l'IA viene usata per gestire il personale (es. turnazione automatica, valutazione performance), il dipendente deve essere informato preventivamente.
- 

#### 3. Utilizzo dell'IA nei Procedimenti Amministrativi

La legge italiana chiarisce i confini dell'automazione:

- **Supporto, non sostituzione**: L'IA può istruire la pratica, ma la decisione finale deve avere una "mediazione umana".
  - **Il Principio di Non-Esclusività**: Nessun cittadino può essere privato di un diritto o subire un effetto giuridico basato *solo* su un algoritmo senza che un funzionario ne abbia convalidato il percorso logico. Vedi art. 22 GDPR
  - **Motivazione dell'Atto**: Se l'IA ha contribuito a formare la decisione, la motivazione del provvedimento (ex L. 241/90) deve darne conto.
- 

#### 4. Sanzioni e Responsabilità

La Legge 132/2025 non scherza:

- Prevede sanzioni amministrative pesanti per gli enti che utilizzano sistemi "ad alto rischio" senza le necessarie valutazioni d'impatto (FRIA - *Fundamental Rights Impact Assessment*).
- Ribadisce che il fornitore e l'utilizzatore (il Comune) sono solidalmente responsabili se non hanno configurato correttamente il sistema secondo i principi di *privacy* ed *ethics by design*.

## **INTELLIGENZA ARTIFICIALE NELLA P.A.**

L'intelligenza artificiale sta trasformando il lavoro nella Pubblica Amministrazione, modificando processi, ruoli e competenze. L'IA non viene presentata come semplice tecnologia, ma come un fattore che ridisegna l'organizzazione stessa.

### **Pervasività dell'IA nella PA**

L'IA entra in sempre più attività quotidiane, automatizzando compiti ripetitivi e supportando decisioni complesse. Questo porta a ripensare flussi di lavoro, responsabilità e modalità di erogazione dei servizi.

### **Impatto sui modelli organizzativi**

L'introduzione dell'IA richiede nuove strutture interne, maggiore integrazione tra uffici e una governance più solida dei dati. Cambiano anche i confini tra attività umane e automatizzate.

### **Competenze e formazione**

Cresce la necessità di competenze digitali, capacità di interpretare output algoritmici e di gestire strumenti intelligenti. La formazione continua diventa un elemento strategico.

### **Sfide etiche e operative**

L'adozione dell'IA porta con sé questioni legate a trasparenza, responsabilità, privacy e qualità dei dati. La PA deve garantire che l'uso dell'IA sia affidabile, equo e comprensibile ai cittadini.

## **DOMANDE DA PORCI**

1. **"Il Comune può far decidere a un'IA chi riceve il buono pasto, senza che un umano controlli."**
2. **"L'informativa privacy deve citare se il software usa logiche di IA."**
3. **"Se l'IA sbaglia, la colpa è solo dell'azienda che ha venduto il software."**

**Attenzione: la Legge 132/2025** protegge anche la proprietà intellettuale e la cybersicurezza: usare "ChatGPT pubblico" per inserire dati dei cittadini è una violazione gravissima sia della legge IA che del GDPR. Bisogna usare solo strumenti "chiusi" e certificati dall'azienda.

## **Il Principi fondamentali della Legge e ripercussioni sulla PA**

### **1 Il Principio dell'Autonomia Umana (Art. 3)**

La legge italiana ribadisce con forza che l'IA non è un "soggetto", ma uno "strumento".

Il legislatore ha voluto evitare il rischio di "delega tecnologica". L'IA deve essere progettata e utilizzata in modo da non limitare l'autonomia decisionale dell'uomo.

**Per la PA:** Questo significa che un algoritmo di profilazione (es. per l'evasione fiscale) non può mai generare una sanzione automatica. Deve sempre esserci un "human-in-the-loop" che valida l'output.

## 2. La Trasparenza "Rafforzata" (Art. 7 e 8)

Mentre il GDPR parla di "logica del trattamento", la L. 132/2025 va oltre, richiedendo che l'uso dell'IA sia **conoscibile e comprensibile**.

Non basta pubblicare un'informativa. L'Ente deve essere in grado di spiegare *come* i dati sono stati pesati dall'algoritmo. **Spiegabilità!**

La trasparenza non è solo un obbligo legale, ma una difesa tecnica. Se il Comune può spiegare il "perché" di una decisione, il rischio di soccombenza in un ricorso al TAR si riduce drasticamente.

## 3. La Governance Nazionale: Il Ruolo di AgID e ACN

L'Italia ha scelto una struttura duale per la vigilanza, coordinata dalla Presidenza del Consiglio.

- **AgID (Competenza Funzionale):** Si assicura che l'IA nella PA funzioni bene e sia interoperabile.
- **ACN (Competenza Tecnica/Cyber):** Si assicura che l'IA non sia vulnerabile ad attacchi (es. *data poisoning* o manipolazione degli algoritmi).

Questa distinzione chiarisce che la conformità non è solo "privacy", ma anche "sicurezza nazionale" e "efficienza digitale".

Punto di Forza	Criticità / Sfida Operativa
<b>Certezza Giuridica:</b> Finalmente c'è un perimetro chiaro per chi sviluppa software per la PA.	<b>Onere Burocratico:</b> La redazione dei FRIA (Fundamental Rights Impact Assessment) richiede competenze elevate.
<b>Etica by Design:</b> L'obbligo di testare i bias (pregiudizi) prima del rilascio protegge le minoranze.	<b>Costi di Adeguamento:</b> I piccoli Comuni potrebbero faticare ad aggiornare i propri sistemi.
<b>Valorizzazione del Dipendente:</b> La legge punta sulla formazione (Art. 10), ridando dignità al ruolo umano.	<b>Responsabilità:</b> Il confine tra errore umano e difetto del software resta complesso da definire.

L'intelligenza artificiale è un'opportunità di modernizzazione, a patto che il fine ultimo resti il servizio al cittadino e non l'efficientamento fine a se stesso.

## Art. 12 - L'IA nella Sanità e nei Servizi Sociali

Questo articolo è fondamentale per la profilazione. Stabilisce che i sistemi di IA usati per la diagnosi, la cura o l'accesso ai servizi sociali devono essere sottoposti a una **validazione clinica o sociale** preventiva.

Il legislatore teme il "pregiudizio algoritmico" in settori vitali. Per gli impiegati che gestiscono, ad esempio, i **Piani di Zona** o l'assistenza domiciliare, l'Art. 12 impone che i criteri di selezione (punteggi di fragilità) siano trasparenti e non basati su dati discriminatori (es. residenza in quartieri degradati come unico fattore di rischio).

### **Art. 15 - La Trasparenza nei Rapporti con i Cittadini**

L'articolo introduce l'obbligo di segnalare in modo inequivocabile quando un cittadino sta interagendo con un'IA (es. chatbot) o quando un provvedimento è frutto di un'elaborazione algoritmica.

- Non è solo un obbligo di "etichettatura". È una garanzia di **diritto alla difesa**. Se il cittadino sa che un'IA ha istruito la sua pratica, può esercitare il diritto di richiedere l'intervento umano (Art. 22 GDPR).
- **Impatto PA:** Ogni comunicazione ufficiale (lettere, avvisi di accertamento) deve contenere la dicitura: *"Documento elaborato con il supporto di sistemi di Intelligenza Artificiale ai sensi della L. 132/2025"*.

### **Art. 18 - Proprietà Intellettuale e Dati della PA**

Questo articolo affronta il tema dei "dati di addestramento". Stabilisce che i dati prodotti dalla PA italiana non possono essere usati liberamente dai provider di IA per addestrare i propri modelli senza autorizzazione o accordi specifici.

È una norma di sovranità digitale. Impedisce che il patrimonio informativo dei Comuni (dati anagrafici, tributari, urbanistici) diventi "carburante gratuito" per le grandi Big Tech straniere, senza che vi sia un ritorno in termini di sicurezza e controllo per lo Stato.

### **Art. 21 - Cybersicurezza e Resilienza**

In combinato disposto con le direttive dell'ACN, l'articolo impone che i sistemi di IA della PA siano "resilienti".

Un sistema di IA non deve solo essere "bravo" a fare calcoli, deve essere immune ad attacchi di **Adversarial Machine Learning** (tentativi di ingannare l'algoritmo per ottenere vantaggi indebiti, come un sussidio non dovuto).

#### **CICLO DELLE RESPONSABILITÀ**

**1 Valutazione (Pre-deployment):** Verifica se il sistema è ad alto rischio (Art. 6 AI Act).

**2 Impatto (FRIA & DPIA):** Valutazione dei rischi per i diritti fondamentali e la privacy (Art. 35 GDPR + L. 132/2025).

**3 Informazione:** Comunicazione al cittadino dell'uso dell'IA (Art. 15 L. 132/2025).

**4 Monitoraggio:** Supervisione umana costante (Human-in-the-loop).

**5 Audit:** Conservazione dei log e della documentazione tecnica per eventuali controlli di AgID.

la Legge 132/2025 trasforma il dipendente pubblico da "esecutore" a "validatore". L'IA fa il lavoro pesante, l'impiegato esercita il potere amministrativo.

### III AgID: Le Regole del Gioco per la PA

AgID agisce come il "braccio operativo". I suoi interventi mirano a far sì che i sistemi di IA siano sicuri, interoperabili e utili.

**Linee Guida per l'adozione dell'IA nella PA (Febbraio 2025):** È l'atto più importante. AgID stabilisce che le PA devono mappare i propri sistemi di IA secondo le **classi di rischio dell'AI Act**.

Introduce l'obbligo di valutare l'**impatto energetico e ambientale** dell'IA (sostenibilità).

Prevede che ogni sistema IA "ad alto impatto" debba avere una documentazione tecnica che permetta di risalire alla responsabilità umana in ogni fase.

**Piano Triennale per l'Informatica nella PA (Aggiornamento 2024-2026):** AgID ha inserito obiettivi specifici per l'uso dell'IA generativa nel back-office (es. classificazione atti e supporto al cittadino).

Promuove il **riuso**: se un Comune sviluppa un buon sistema di IA (es. per i tributi), questo deve essere messo a disposizione degli altri enti tramite il catalogo dei software di AgID.

---

### Il Garante Privacy: La Tutela dei Diritti

Il Garante interviene quando l'IA "tocca" le persone. Il suo approccio è basato sulla prevenzione della discriminazione e sulla trasparenza.

#### Provvedimenti su Algoritmi e Lavoro Pubblico (Gennaio 2025):

- Il Garante ha ribadito che l'uso di algoritmi per valutare le performance dei dipendenti o per decidere turnazioni deve essere **trasparente**. Il dipendente deve poter conoscere i parametri usati dalla macchina.

**Decalogo sull'IA Generativa (2024/2025):** A seguito del caso ChatGPT, il Garante ha emanato prescrizioni rigide: chi usa IA deve garantire che i dati non vengano usati per "auto-addestramento" senza consenso (molto importante per Kibernetes: i dati dei cittadini non devono mai uscire dal perimetro sicuro dell'ente).

#### Provvedimenti contro il "Web Scraping" (Ottobre 2025):

Ha imposto restrizioni tecniche per impedire che software di IA "peschino" dati dai siti della PA per profilare i cittadini senza base giuridica.

<b>Caratteristica</b>	<b>AgID (Efficienza Tecnica)</b>	<b>Garante Privacy (Diritto della Persona)</b>
<b>Obiettivo</b>	Modernizzare la PA e standardizzare i sistemi.	Proteggere i dati e prevenire discriminazioni.
<b>Focus Principale</b>	Sicurezza informatica, interoperabilità, AI Act.	Rispetto del GDPR, trasparenza, non-profilazione.
<b>Cosa controlla?</b>	Che il software sia a norma tecnica e non sprechi risorse.	Che il trattamento dei dati sia lecito e non opaco.
<b>Documento chiave</b>	Linee Guida IA nella PA (2025).	DPIA (Valutazione Impatto) e Decalogo IA.
<b>Autorità di riferimento</b>	Designata dall'AI Act (Nazionale).	Autorità di controllo ex Art. 51 GDPR.

## FASE OPERATIVA

### Checklist di Conformità IA per la Pubblica Amministrazione

#### 1. Inquadramento e Rischio (AI Act & L. 132/2025)

- **Classificazione:** Abbiamo identificato se il sistema è ad "Alto Rischio" (es. selezione personale, sussidi, istruzione, accesso a servizi pubblici)?
- **Divieti:** Il sistema evita pratiche vietate (es. punteggio sociale, riconoscimento delle emozioni sul posto di lavoro, identificazione biometrica non autorizzata)?
- **Finalità Pubblica:** È chiaro l'interesse pubblico perseguito? (Art. 1 L. 132/2025).

#### 2. Protezione Dati e Profilazione (GDPR)

- **DPIA (Valutazione Impatto):** È stata aggiornata la DPIA includendo i rischi specifici dell'algoritmo (opacità, errori, bias)?
- **Base Giuridica:** Esiste una norma di legge o regolamento che autorizza questo specifico trattamento automatizzato?
- **Profilazione:** Se il sistema profila i cittadini, è stata prevista una procedura per gestire il diritto di opposizione?

### 3. Trasparenza e Relazione col Cittadino (Art. 15 L. 132/2025)

- **Etichettatura:** Le comunicazioni prodotte dall'IA contengono la dicitura "*Documento assistito da sistemi di IA*"?
- **Informativa:** Il cittadino è informato che sta interagendo con un'IA o che una decisione lo riguarda in quanto frutto di elaborazione algoritmica?
- **Spiegabilità:** Se il cittadino chiede "perché ho avuto questo punteggio?", l'operatore è in grado di estrarre dal sistema la logica della decisione?

### 4. Supervisione Umana (Human-in-the-loop)

- **Validazione Finale:** Esiste un passaggio obbligatorio in cui un funzionario umano approva, firma o convalida l'output dell'IA? (Art. 14 L. 132/2025).
- **Capacità di Intervento:** Il dipendente ha la formazione e il potere tecnico di ignorare o correggere il suggerimento della macchina?
- **Log e Audit:** Il sistema registra chi ha validato la decisione e se sono state apportate modifiche umane all'output?

### 5. Qualità e Sicurezza (AgID & ACN)

- **Data Quality:** I dati di addestramento o di input sono esatti, aggiornati e privi di pregiudizi (bias) statistici?
- **Conformità Tecnica:** Il fornitore (es. Kibernetes) ha fornito la documentazione tecnica richiesta dalle Linee Guida AgID 2025?
- **Cybersicurezza:** Il sistema è protetto contro tentativi di manipolazione dei dati o degli algoritmi?

Le linee guida di AgID (Agenzia per l'Italia Digitale) sull'Intelligenza Artificiale sono un pilastro fondamentale del **Piano Triennale per l'Informatica nella PA 2024-2026**.

Proprio di recente, a febbraio 2025, AgID ha rilasciato la bozza ufficiale delle **"Linee Guida per l'adozione dell'IA nella Pubblica Amministrazione"** (Determinazione n. 17/2025), aprendo una consultazione pubblica conclusasi a marzo 2025.

Ecco i punti chiave e i principi stabiliti da AgID:

## 1. Principi Fondamentali (Il Decalogo)

AgID ha delineato una strategia basata sull'approccio "antropocentrico", in linea con l'AI Act europeo. I principi cardine includono:

- **Trasparenza e Spiegabilità:** I cittadini devono poter capire come e perché un sistema di IA ha preso una determinata decisione.
- **Supervisione Umana (Human-in-the-loop):** L'IA non deve mai sostituire completamente il giudizio umano, specialmente in decisioni che impattano i diritti dei cittadini.
- **Non Discriminazione:** I dataset utilizzati devono essere privi di bias per evitare trattamenti iniqui.
- **Sicurezza e Cybersicurezza:** I sistemi devono essere resilienti agli attacchi e proteggere i dati sensibili.

## 2. Obiettivi Strategici

L'adozione dell'IA nella PA italiana mira a tre obiettivi principali:

1. **Efficienza Operativa:** Automatizzare compiti ripetitivi per liberare risorse umane verso attività a maggior valore aggiunto.
2. **Miglioramento dei Servizi:** Offrire risposte più rapide e personalizzate ai cittadini (es. chatbot avanzati, analisi predittiva per la salute).
3. **Supporto alle Decisioni:** Utilizzare l'analisi dei dati per politiche pubbliche basate su evidenze (data-driven).

## 3. Classificazione del Rischio

Le linee guida recepiscono la classificazione dell'**AI Act**, distinguendo tra:

- **Rischio inaccettabile:** Pratiche vietate (es. social scoring).
- **Alto rischio:** Sistemi che impattano istruzione, lavoro o infrastrutture critiche (richiedono requisiti severi e certificazioni).
- **Rischio limitato/minimo:** Sistemi come i chatbot, dove vige principalmente l'obbligo di trasparenza (l'utente deve sapere che sta interagendo con un'IA).

## 4. Governance e Competenze

AgID sottolinea che l'IA non è solo una sfida tecnologica, ma organizzativa:

- **Ruolo del RTD:** Il Responsabile per la Transizione Digitale diventa la figura chiave per governare l'adozione dell'IA in ogni ente.

- **Formazione:** Viene data enorme importanza al *reskilling* dei dipendenti pubblici per comprendere e gestire correttamente questi strumenti.
- **Acquisti Pubblici:** AgID fornisce indicazioni su come le PA devono acquistare soluzioni di IA, privilegiando la sovranità dei dati e l'interoperabilità.

Secondo le direttive AgID aggiornate al **2026** e il **Piano Triennale 2024-2026**, ecco come gli enti locali devono muoversi:

---

## 1. La Governance Locale: Il Ruolo del RTD

Il **Responsabile per la Transizione Digitale (RTD)** è la figura centrale. Per i Comuni, le linee guida stabiliscono che:

- Il RTD deve coordinare la valutazione dell'impatto algoritmico (DPIA) per ogni nuovo sistema di IA.
- Nei **piccoli Comuni**, AgID promuove forme di **gestione associata** (Unioni di Comuni) per condividere esperti e costi di implementazione.
- È obbligatorio censire i sistemi di IA utilizzati all'interno del censimento del patrimonio ICT dell'ente.

## 2. Casi d'Uso Ammessi e Prioritari

AgID ha individuato ambiti specifici dove i Comuni possono (e dovrebbero) applicare l'IA:

- **Servizi al Cittadino:** Chatbot e assistenti virtuali per fornire informazioni h24 su tributi, scadenze e procedure anagrafiche.
- **Gestione del Territorio:** Sistemi di visione artificiale per il monitoraggio del traffico, dello stato del manto stradale o per la gestione ottimizzata dei rifiuti.
- **Analisi dei Dati Urbani:** Utilizzo di IA per prevedere i flussi turistici o pianificare i servizi di trasporto locale (Smart City).

## 3. Il "Principio di Precauzione" e Divieti

I Comuni devono prestare particolare attenzione ai sistemi ad **Alto Rischio** secondo l'AI Act:

- **Polizia Locale:** È vietato l'uso di sistemi di identificazione biometrica remota in tempo reale in spazi pubblici (salvo eccezioni strettissime di sicurezza nazionale).
- **Servizi Sociali:** L'uso di algoritmi per decidere l'assegnazione di sussidi o benefici deve essere accompagnato da una spiegazione chiara del punteggio (niente "scatole nere").
- **Social Scoring:** È categoricamente vietato ai Comuni utilizzare l'IA per valutare l'affidabilità sociale dei cittadini basata sui loro comportamenti.

## 4. Procurement (Acquisto dell'IA)

Le linee guida AgID forniscono indicazioni precise su come scrivere i bandi di gara:

- **Clausole di Trasparenza:** I fornitori devono garantire l'accesso al codice o, quanto meno, la spiegabilità dell'output.

- **Sovranità dei Dati:** I dati dei cittadini residenti devono risiedere in infrastrutture cloud qualificate (PSN - Polo Strategico Nazionale) o certificate AgID.
- 

## Supporto per i Piccoli Comuni

Se fai parte di un ente locale di piccole dimensioni, sappi che AgID e Formez hanno lanciato il progetto **"FAST Piccoli Comuni"**. Questo programma offre:

1. **Modelli predefiniti** per i regolamenti comunali sull'uso dell'IA.
2. **Laboratori di sperimentazione (Sandbox)** per testare soluzioni di IA generativa per la stesura di atti amministrativi senza rischi legali.

**Nota Bene:** Con l'entrata in vigore della **Legge 132/2025**, i Comuni sono tenuti a pubblicare sul proprio sito istituzionale un elenco aggiornato dei sistemi di IA che interagiscono con il pubblico.

## Conversazione con Gemini

Hai detto

Ciao domani sarò di nuovo docente in un corso sul gdpr indirizzato agli impiegati della Kibernetes di palermo. Vorrei approfondire per i miei allievi il regolamento europeo AI act e la legge italiana sull'intelligenza artificiale evidenziando due aspetti: i punti di contatto con il gdpr e l'utilizzo dell'IA nella pubblica amministrazione. Puoi fornirmi traccia e contenuti in dettaglio?

## Gemini ha detto

Certamente. Per la tua docenza agli impiegati di **Kibernetes Palermo**, azienda che vive quotidianamente i processi di digitalizzazione della PA (dalla gestione documentale ai servizi demografici), è fondamentale declinare l'AI Act e la normativa italiana non come "teoria", ma come un'estensione operativa del GDPR che già conoscono.

Ecco una traccia strutturata per il tuo intervento, aggiornata alla **Legge 132/2025** (la legge quadro italiana sull'IA).

---

## 1. Il Quadro Normativo: AI Act e Legge Italiana

L'intelligenza artificiale non sostituisce il GDPR, ma vi si innesta sopra.

- **AI Act (Regolamento UE 2024/1689):** Disciplina il "prodotto" e il suo rischio. Si concentra su **cosa** fa la macchina.
  - **Legge Italiana (L. 132/2025):** Integra l'AI Act definendo la governance nazionale (AgID e ACN come autorità di vigilanza) e norme specifiche per settori critici come la PA e il lavoro.
- 

## 2. Punti di Contatto tra AI Act e GDPR

Per un impiegato che si occupa di dati, i due regolamenti sono "vasi comunicanti".

Caratteristica	GDPR (Dati Personali)	AI Act (Sistemi di IA)
<b>Focus</b>	Protezione della persona fisica.	Sicurezza e affidabilità del sistema.
<b>Analisi del Rischio</b>	<b>DPIA</b> (Valutazione d'impatto sulla protezione dati).	<b>FRIA</b> (Fundamental Rights Impact Assessment) per sistemi ad alto rischio.
<b>Principio Cardine</b>	<i>Privacy by Design.</i>	<i>Ethics by Design</i> e Trasparenza.
<b>Ruoli Soggettivi</b>	Titolare / Responsabile.	Provider (Fornitore) / Deployer (Utilizzatore).

**Il concetto chiave per l'aula:** Un sistema di IA che analizza dati dei cittadini deve essere conforme a entrambi. Se l'IA è "sicura" ma usa dati senza base giuridica, è illecita per il GDPR. Se i dati sono corretti ma l'algoritmo è "opaco" o discriminatorio, è illecita per l'AI Act.

### 3. L'IA nella Pubblica Amministrazione

Questo è il cuore per i dipendenti Kibernetes, dato il loro ruolo di supporto agli Enti Locali.

#### A. Il Principio di Non-Sostituzione (Art. 14 L. 132/2025)

L'IA nella PA ha una funzione esclusivamente **strumentale e di supporto**.

- **Decisione Umana:** Un atto amministrativo o un provvedimento non può essere adottato *esclusivamente* da un'IA. Deve esserci sempre la supervisione e la firma di un funzionario umano (responsabile del procedimento).
- **Motivazione:** Il cittadino ha il diritto di conoscere la "logica" dietro una decisione assistita da IA.

#### B. Casi d'Uso Tipici per la PA

1. **Semplificazione del linguaggio:** Tradurre il "burocratese" in testi chiari per il cittadino.
2. **Back-office:** Classificazione automatica delle PEC o estrazione dati da documenti cartacei digitalizzati.
3. **Assistenti Virtuali (Chatbot):** Supporto h24 per fornire informazioni su tributi o scadenze (es. Suite KSD di Kibernetes).

#### C. I Sistemi ad "Alto Rischio"

Molti sistemi usati nella PA ricadono nella categoria ad alto rischio dell'AI Act:

- Sistemi per l'accesso a servizi pubblici e prestazioni sociali.
- Sistemi per il reclutamento e la gestione del personale (selezione candidati).

- Sistemi di identificazione biometrica (con divieti e deroghe molto stringenti).
- 

#### 4. Obblighi Operativi per i Dipendenti

Cosa cambia da domani sulla scrivania?

1. **Dovere di Informativa:** Se l'Ente usa un'IA per interagire con il cittadino (es. un bot), deve dichiararlo esplicitamente.
  2. **Verifica dell'Output:** Il dipendente non deve fidarsi ciecamente dell'IA. L'errore algoritmico ("allucinazione") non esonera il funzionario dalla responsabilità del provvedimento.
  3. **Data Quality:** L'accuratezza dei dati in ingresso (già prevista dal GDPR) diventa vitale: dati sporchi generano decisioni discriminatorie (bias).
- 

#### 5. Sintesi per l'Aula (Slide finale)

"L'IA è il motore, i dati sono il carburante. Il GDPR controlla che il carburante sia prelevato legalmente; l'AI Act controlla che il motore non esploda e non vada fuori strada. Ma alla guida resta sempre il funzionario pubblico."

---

**Ti serve che approfondisca un caso d'uso specifico (es. gestione tributi o anagrafe) o che prepari un breve quiz di verifica per i tuoi allievi?**

Hai detto

vorrei che tu evidenziassi gli utilizzi nella pubblica amministrazione e quelli già in uso. Mi serve anche evidenziare i rischi legati a processi automatizzati di profilazione

**Gemini ha detto**

Per la tua lezione a **Kibernetes Palermo**, è fondamentale mostrare che l'IA non è "il futuro", ma una realtà già operativa negli uffici pubblici. Tuttavia, questa operatività porta con sé il rischio della **profilazione algoritmica**, un tema sensibilissimo per il GDPR.

Ecco l'approfondimento dettagliato sui casi d'uso e sui rischi di profilazione.

---

#### 1. L'IA già in uso nella PA Italiana (Casi Reali)

Gli impiegati devono sapere che molti strumenti che già utilizzano (o che vedranno presto) integrano logiche di IA.

##### A. Supporto Documentale e Relazione col Cittadino

- **Smistamento Automatico PEC:** Sistemi che leggono l'oggetto e il contenuto delle PEC in arrivo per assegnarle automaticamente all'ufficio competente (es. Protocollo informatico avanzato).
- **Chatbot e Assistenti Virtuali:** L'**INPS** e l'**Agenzia delle Entrate** utilizzano già assistenti (come *Sofia* o *mAigov*) che usano il linguaggio naturale (NLP) per guidare l'utente tra i servizi.

- **Semplificazione del Linguaggio:** Strumenti usati per riscrivere determine e atti amministrativi complessi in un linguaggio più accessibile (secondo le direttive AgID 2024-2026).

## B. Contrasto all'Evasione e Controlli (Profilazione "Buona")

- **Agenzia delle Entrate (VeRa):** L'algoritmo di "Verifica Rapporti" incrocia i dati dei conti correnti con le dichiarazioni dei redditi per individuare scostamenti sospetti.
- **Monitoraggio Ambientale:** Uso di droni e immagini satellitari analizzate da IA per individuare abusi edilizi o discariche abusive nei Comuni.

## C. Sanità e Welfare

- **SINFONIA (Regione Campania):** Un ecosistema che analizza i dati sanitari per prevedere le necessità di cura dei pazienti cronici e ottimizzare le liste d'attesa.
- **Inail:** Utilizzo di modelli predittivi per analizzare i rischi di infortuni sul lavoro in specifici settori industriali.

---

## 2. I Rischi della Profilazione Automatizzata

Qui entra in gioco il **GDPR (Art. 22)** e il nuovo **AI Act**. La profilazione è il trattamento automatizzato di dati personali per valutare aspetti della persona (rendimento, situazione economica, salute, preferenze).

### I Tre Grandi Rischi per il Dipendente Pubblico:

1. **L'Effetto "Scatola Nera" (Opacità):** Se un'IA decide chi ha diritto a un sussidio o chi deve subire un accertamento fiscale, e l'impiegato non sa *perché* l'ha deciso, si viola il principio di **Trasparenza**.
  - *Rischio:* Ricorsi di massa dei cittadini per "difetto di motivazione" dell'atto amministrativo.
2. **Bias e Discriminazione Algoritmica:** Gli algoritmi imparano dai dati storici. Se i dati del passato contengono pregiudizi (es. discriminazioni territoriali o di genere), l'IA li amplificherà.
  - *Esempio:* Un software di selezione del personale che scarta sistematicamente candidati di una certa zona geografica perché "storicamente" meno stabili.
3. **Il "Determinismo" Sociale:** Profilare un cittadino come "soggetto a rischio evasione" solo sulla base di modelli statistici può creare una sorta di "pre-giudizio digitale" che limita le sue libertà prima ancora che abbia commesso un'infrazione.

---

## 3. Come Difendersi: Le Tutele del GDPR e AI Act

In aula, sottolinea che il dipendente ha un ruolo di **"Human-in-the-loop"** (supervisione umana).

- **Diritto all'Intervento Umano (Art. 22 GDPR):** Il cittadino ha il diritto di non essere sottoposto a una decisione basata *unicamente* sul trattamento automatizzato. Un umano deve sempre poter rivedere e cambiare la decisione dell'IA.
- **Data Quality:** L'impiegato deve assicurarsi che i dati inseriti nei sistemi siano esatti. Se il dato è sbagliato, la profilazione sarà ingiusta.

- **Informativa Chiara:** Non basta dire "usiamo l'IA". Bisogna spiegare al cittadino che è in corso una profilazione e quali sono le conseguenze previste.
- 

### **Proposta di esercitazione per i tuoi allievi:**

*"Immaginate che il Comune decida di usare un'IA per assegnare i posti negli asili nido basandosi sulla profilazione del reddito e della composizione familiare. Quali informazioni dovremmo scrivere nell'informativa privacy per essere in regola con il GDPR e l'AI Act?"*

### **Ti andrebbe se preparassi uno schema di questa informativa-tipo da distribuire come materiale didattico?**

Hai detto

si grazie

### **Gemini ha detto**

Ecco uno schema pratico di **Informativa Privacy "Ibrida" (GDPR + AI Act)**.

Puoi distribuirlo come esempio di come un Comune o un ente della PA dovrebbe comunicare in modo trasparente l'uso di sistemi di profilazione algoritmica (prendendo come esempio il caso degli asili nido o dei sussidi sociali).

---

## **Modello di Informativa: Utilizzo di Sistemi di IA e Profilazione**

### **Oggetto: Trattamento dati per la formazione di graduatorie assistite da Intelligenza Artificiale**

#### **1. Chi tratta i tuoi dati? (Titolare del Trattamento)**

Il Comune di [Nome Comune], con sede in [Indirizzo], in qualità di Titolare del trattamento.

#### **2. Che cos'è il sistema di IA utilizzato? (Trasparenza AI Act)**

Per la gestione delle istanze, l'Ente utilizza il software **[Nome Software]**, un sistema di Intelligenza Artificiale classificato come **"ad alto rischio"** ai sensi dell'AI Act (Reg. UE 2024/1689), poiché impiegato per la valutazione dell'accesso a servizi pubblici essenziali.

- **Logica del sistema:** L'algoritmo analizza i dati dichiarati (ISEE, composizione nucleo familiare, distanza residenza, situazioni di disabilità) per calcolare un punteggio di priorità basato sui criteri del Regolamento Comunale n. [X].

#### **3. Perché profilizziamo i tuoi dati? (Base Giuridica GDPR)**

La profilazione è necessaria per l'esecuzione di un **compito di interesse pubblico** (Art. 6.1, lett. e, GDPR). Il sistema confronta i profili dei richiedenti per garantire equità e oggettività nella distribuzione delle risorse limitate, eliminando possibili errori umani di calcolo.

#### **4. Come avviene la decisione? (Intervento Umano - Art. 22 GDPR)**

**Importante:** La decisione **non è interamente automatizzata**.

- L'IA genera una "proposta di graduatoria".
- Un funzionario responsabile (Umano) verifica la coerenza dei dati e valida il risultato finale.

- L'intervento umano garantisce la possibilità di correggere eventuali anomalie generate dall'algoritmo.

## 5. Quali sono i rischi e come li gestiamo?

- **Rischio di Bias (Pregiudizio):** Il sistema è stato sottoposto a test di accuratezza per evitare discriminazioni basate su origine, religione o quartiere di residenza.
- **Data Quality:** Utilizziamo solo dati certificati provenienti dall'Anagrafe Nazionale (ANPR) e dall'INPS per alimentare il sistema.

## 6. I tuoi diritti

Oltre ai diritti standard (accesso, rettifica, cancellazione), ai sensi dell'Art. 22 del GDPR e dell'AI Act, hai il diritto di:

- Ottenere una **spiegazione chiara** sulla logica che ha portato al tuo punteggio.
- Richiedere l'**intervento umano** per la revisione della tua pratica.
- Contestare la decisione se ritieni che l'IA abbia interpretato erroneamente la tua situazione familiare.

---

## Consigli per la tua lezione a Palermo:

1. **Sottolinea la "Spiegabilità":** Spiega agli allievi che non basta dire "l'ha deciso il computer". Se un cittadino bussa allo sportello chiedendo perché è sceso in graduatoria, l'impiegato deve essere in grado di spiegare quali parametri hanno influenzato il punteggio.
2. **Focus sulla Responsabilità:** Ricorda loro che la firma sul provvedimento finale è la loro, non del fornitore del software. L'IA è un **parere istruttorio**, non una sentenza.
3. **Il ruolo di Kibernetes:** In quanto partner tecnologico, Kibernetes ha il compito di fornire sistemi "Auditabili", ovvero sistemi che permettano all'impiegato di ricostruire il ragionamento fatto dall'IA in qualsiasi momento.

## Vuoi che ti prepari anche 3-4 domande "trabocchetto" per un test finale da sottoporre agli impiegati?

Hai detto

LEGGE 23 settembre 2025, n. 132 - Normattiva

### Gemini ha detto

Ottima scelta citare la **Legge n. 132/2025** (la cosiddetta "Legge Quadro sull'IA"). Per la tua docenza a Kibernetes, questo è il tassello che chiude il cerchio tra la teoria europea (AI Act) e la pratica amministrativa italiana.

Ecco i punti salienti della legge da trasmettere ai tuoi allievi, con un focus operativo su **responsabilità e trasparenza**.

---

## 1. Governance e Vigilanza (Chi controlla?)

La Legge 132/2025 designa le autorità nazionali competenti per l'applicazione dell'AI Act:

- **AgID (Agenzia per l'Italia Digitale):** Si occupa della promozione dell'innovazione e della verifica della conformità tecnica. È l'interlocutore principale per la PA.
  - **ACN (Agenzia per la Cybersicurezza Nazionale):** Vigilanza sugli aspetti di sicurezza informatica dei sistemi di IA.
  - **Garante Privacy:** Resta l'autorità suprema per quanto riguarda l'impatto dei sistemi di IA sui dati personali e sulla profilazione.
- 

## 2. L'IA nel Lavoro Pubblico (Art. 10 e segg.)

Questa parte è vitale per i dipendenti di Kibernetes e i loro clienti (Enti Locali):

- **Obbligo di Formazione:** La legge impone alle PA di formare il personale sull'uso etico e critico dell'IA. (La tua docenza di domani assolve proprio a questo precetto legislativo!).
  - **Trasparenza verso il Lavoratore:** Se l'IA viene usata per gestire il personale (es. turnazione automatica, valutazione performance), il dipendente deve essere informato preventivamente.
- 

## 3. Utilizzo dell'IA nei Procedimenti Amministrativi

La legge italiana chiarisce i confini dell'automazione:

- **Supporto, non sostituzione:** L'IA può istruire la pratica, ma la decisione finale deve avere una "mediazione umana".
  - **Il Principio di Non-Esclusività:** Nessun cittadino può essere privato di un diritto o subire un effetto giuridico basato *solo* su un algoritmo senza che un funzionario ne abbia convalidato il percorso logico.
  - **Motivazione dell'Atto:** Se l'IA ha contribuito a formare la decisione, la motivazione del provvedimento (ex L. 241/90) deve darne conto.
- 

## 4. Sanzioni e Responsabilità

La Legge 132/2025 non scherza:

- Prevede sanzioni amministrative pesanti per gli enti che utilizzano sistemi "ad alto rischio" senza le necessarie valutazioni d'impatto (**FRIA - Fundamental Rights Impact Assessment**).
  - Ribadisce che il fornitore (es. Kibernetes) e l'utilizzatore (il Comune) sono solidalmente responsabili se non hanno configurato correttamente il sistema secondo i principi di *privacy* ed *ethics by design*.
- 

## Esercizio Rapido: "Vero o Falso" per la tua aula

Per testare l'attenzione dopo aver spiegato la L. 132/2025:

1. "Il Comune può far decidere a un'IA chi riceve il buono pasto, senza che un umano controlli."

- *Risposta: Falso.* La L. 132/2025 impone la supervisione umana per atti che producono effetti giuridici.

## 2. "L'informativa privacy deve citare se il software usa logiche di IA."

- *Risposta: Vero.* È un obbligo di trasparenza previsto sia dal GDPR che dalla nuova legge italiana.

## 3. "Se l'IA sbaglia, la colpa è solo dell'azienda che ha venduto il software."

- *Risposta: Falso.* Il Titolare (l'Ente) è responsabile della scelta del fornitore e del corretto utilizzo del sistema.

---

### Un ultimo suggerimento per Palermo

Kibernetes gestisce molti dati sensibili. Ricorda ai tuoi allievi che la **Legge 132/2025** protegge anche la proprietà intellettuale e la cybersicurezza: usare "ChatGPT pubblico" per inserire dati dei cittadini è una violazione gravissima sia della legge IA che del GDPR. Bisogna usare solo strumenti "chiusi" e certificati dall'azienda.

**Ti servirebbe una "checklist" finale da lasciare agli allievi per verificare se un processo IA che intendono attivare è a norma?**

Hai detto

puoi elaborare un commento alla legge?

### Gemini ha detto

Certamente. Commentare la **Legge 23 settembre 2025, n. 132** significa analizzare come l'Italia abbia deciso di "mettere a terra" i principi generali dell'AI Act europeo, adattandoli alla specificità del nostro ordinamento amministrativo e costituzionale.

Per la tua docenza, puoi strutturare il commento su tre pilastri critici: **Antropocentrismo, Accountability e Trasparenza Amministrativa.**

---

### Commento alla Legge n. 132/2025: "L'Umano al Centro"

#### 1. Il Principio dell'Autonomia Umana (Art. 3)

La legge italiana ribadisce con forza che l'IA non è un "soggetto", ma uno "strumento".

- **Commento:** Il legislatore ha voluto evitare il rischio di "delega tecnologica". L'IA deve essere progettata e utilizzata in modo da non limitare l'autonomia decisionale dell'uomo.
- **Per la PA:** Questo significa che un algoritmo di profilazione (es. per l'evasione fiscale) non può mai generare una sanzione automatica. Deve sempre esserci un "human-in-the-loop" che valida l'output.

#### 2. La Trasparenza "Rafforzata" (Art. 7 e 8)

Mentre il GDPR parla di "logica del trattamento", la L. 132/2025 va oltre, richiedendo che l'uso dell'IA sia **conoscibile e comprensibile.**

- **Commento:** Non basta pubblicare un'informativa. L'Ente deve essere in grado di spiegare *come* i dati sono stati pesati dall' algoritmo.
- **Rilevanza per Kibernetes:** La trasparenza non è solo un obbligo legale, ma una difesa tecnica. Se il Comune può spiegare il "perché" di una decisione, il rischio di soccombenza in un ricorso al TAR si riduce drasticamente.

### 3. La Governance Nazionale: Il Ruolo di AgID e ACN

L'Italia ha scelto una struttura duale per la vigilanza, coordinata dalla Presidenza del Consiglio.

- **AgID (Competenza Funzionale):** Si assicura che l'IA nella PA funzioni bene e sia interoperabile.
- **ACN (Competenza Tecnica/Cyber):** Si assicura che l'IA non sia vulnerabile ad attacchi (es. *data poisoning* o manipolazione degli algoritmi).
- **Commento:** Questa distinzione chiarisce che la conformità non è solo "privacy", ma anche "sicurezza nazionale" e "efficienza digitale".

---

#### Punti di Forza e Criticità (Per il dibattito in aula)

Punto di Forza

Criticità / Sfida Operativa

**Certezza Giuridica:** Finalmente c'è un perimetro chiaro per chi sviluppa software per la PA.

**Onere Burocratico:** La redazione dei FRIA (Fundamental Rights Impact Assessment) richiede competenze elevate.

**Etica by Design:** L'obbligo di testare i bias (pregiudizi) prima del rilascio protegge le minoranze.

**Costi di Adeguamento:** I piccoli Comuni potrebbero faticare ad aggiornare i propri sistemi.

**Valorizzazione del Dipendente:** La legge punta sulla formazione (Art. 10), ridando dignità al ruolo umano.

**Responsabilità:** Il confine tra errore umano e difetto del software resta complesso da definire.

---

#### Conclusione del Commento

La **L. 132/2025** non deve essere vista come un freno all'innovazione, ma come il "manuale d'istruzioni" per un'innovazione sicura. Per un dipendente della PA, la legge è uno scudo: definisce cosa può fare (usare l'IA per velocizzare il lavoro) e cosa non deve fare (lasciare che l'IA decida al posto suo).

**Citazione chiave per la slide:** *"L'intelligenza artificiale è un'opportunità di modernizzazione, a patto che il fine ultimo resti il servizio al cittadino e non l'efficientamento fine a se stesso."*

---

**Prossimo passo consigliato:**

**Ti servirebbe che riassumessi queste riflessioni in una "Mappa Concettuale" o in uno schema a punti da inserire nelle tue dispense per gli allievi di Kibernetes?**

Hai detto

vorrei che continuassi a commentare anche gli altri articoli della norma

### **Gemini ha detto**

Certamente. Proseguiamo con l'analisi ragionata degli altri pilastri della **Legge n. 132/2025**, focalizzandoci sugli articoli che hanno un impatto diretto sull'operatività quotidiana di una società come Kibernetes e dei suoi interlocutori nella PA.

---

## **Analisi di dettaglio degli articoli chiave (L. 132/2025)**

### **Art. 12 - L'IA nella Sanità e nei Servizi Sociali**

Questo articolo è fondamentale per la profilazione. Stabilisce che i sistemi di IA usati per la diagnosi, la cura o l'accesso ai servizi sociali devono essere sottoposti a una **validazione clinica o sociale** preventiva.

- **Commento:** Il legislatore teme il "pregiudizio algoritmico" in settori vitali. Per gli impiegati che gestiscono, ad esempio, i **Piani di Zona** o l'assistenza domiciliare, l'Art. 12 impone che i criteri di selezione (punteggi di fragilità) siano trasparenti e non basati su dati discriminatori (es. residenza in quartieri degradati come unico fattore di rischio).

### **Art. 15 - La Trasparenza nei Rapporti con i Cittadini**

L'articolo introduce l'obbligo di segnalare in modo inequivocabile quando un cittadino sta interagendo con un'IA (es. chatbot) o quando un provvedimento è frutto di un'elaborazione algoritmica.

- **Commento:** Non è solo un obbligo di "etichettatura". È una garanzia di **diritto alla difesa**. Se il cittadino sa che un'IA ha istruito la sua pratica, può esercitare il diritto di richiedere l'intervento umano (Art. 22 GDPR).
- **Impatto PA:** Ogni comunicazione ufficiale (lettere, avvisi di accertamento) deve contenere la dicitura: *"Documento elaborato con il supporto di sistemi di Intelligenza Artificiale ai sensi della L. 132/2025"*.

### **Art. 18 - Proprietà Intellettuale e Dati della PA**

Questo articolo affronta il tema dei "dati di addestramento". Stabilisce che i dati prodotti dalla PA italiana non possono essere usati liberamente dai provider di IA per addestrare i propri modelli senza autorizzazione o accordi specifici.

- **Commento:** È una norma di sovranità digitale. Impedisce che il patrimonio informativo dei Comuni (dati anagrafici, tributari, urbanistici) diventi "carburante gratuito" per le grandi Big Tech straniere, senza che vi sia un ritorno in termini di sicurezza e controllo per lo Stato.

### **Art. 21 - Cybersicurezza e Resilienza**

In combinato disposto con le direttive dell'ACN, l'articolo impone che i sistemi di IA della PA siano "resilienti".

- **Commento:** Un sistema di IA non deve solo essere "bravo" a fare calcoli, deve essere immune ad attacchi di **Adversarial Machine Learning** (tentativi di ingannare l'algoritmo per ottenere vantaggi indebiti, come un sussidio non dovuto).

---

## Schema di Sintesi: Il Ciclo della Responsabilità

Per aiutare i tuoi allievi a visualizzare il flusso normativo, puoi utilizzare questo schema che riassume gli obblighi previsti dalla legge:

1. **Valutazione (Pre-deployment):** Verifica se il sistema è ad alto rischio (Art. 6 AI Act).
2. **Impatto (FRIA & DPIA):** Valutazione dei rischi per i diritti fondamentali e la privacy (Art. 35 GDPR + L. 132/2025).
3. **Informazione:** Comunicazione al cittadino dell'uso dell'IA (Art. 15 L. 132/2025).
4. **Monitoraggio:** Supervisione umana costante (Human-in-the-loop).
5. **Audit:** Conservazione dei log e della documentazione tecnica per eventuali controlli di AgID.

---

## Riflessione Conclusiva per la Docenza

Il commento complessivo alla legge ci dice che l'Italia ha scelto la via della **"Innovazione Responsabile"**.

Per i dipendenti di Kibernetes, questo significa che lo sviluppo software non finisce con il codice, ma con la **documentazione della conformità**. Un software che funziona bene ma non è documentato secondo la L. 132/2025 è un software che espone l'Ente a rischi legali enormi.

**Consiglio per l'aula:** Chiudi questa sezione ricordando che la Legge 132/2025 trasforma il dipendente pubblico da "esecutore" a "validatore". L'IA fa il lavoro pesante, l'impiegato esercita il potere amministrativo.

**Desideri che prepari una tabella comparativa tra i compiti di AgID e quelli del Garante Privacy da inserire nelle dispense?**

Hai detto

si grazie, puoi anche evidenziare quali sono i provvedimenti in questa materia emanati da agid e dal garante?

**Gemini ha detto**

Certamente. Per la tua docenza è fondamentale distinguere il "chi fa cosa". La **Legge 132/2025** ha creato un sistema a due motori: **AgID** si occupa dell'efficacia e dell'adozione tecnica nella PA, mentre il **Garante Privacy** vigila sui diritti e sulle libertà dei cittadini.

Ecco una sintesi dei provvedimenti e delle linee guida più recenti emessi dalle due Autorità, che puoi inserire direttamente nelle tue dispense.

---

## 1. AgID: Le Regole del Gioco per la PA

AgID agisce come il "braccio operativo". I suoi interventi mirano a far sì che i sistemi di IA siano sicuri, interoperabili e utili.

- **Linee Guida per l'adozione dell'IA nella PA (Febbraio 2025):** \* È l'atto più importante. AgID stabilisce che le PA devono mappare i propri sistemi di IA secondo le **classi di rischio dell'AI Act**.
  - Introduce l'obbligo di valutare l'**impatto energetico e ambientale** dell'IA (sostenibilità).
  - Prevede che ogni sistema IA "ad alto impatto" debba avere una documentazione tecnica che permetta di risalire alla responsabilità umana in ogni fase.
- **Piano Triennale per l'Informatica nella PA (Aggiornamento 2024-2026):** \* AgID ha inserito obiettivi specifici per l'uso dell'IA generativa nel back-office (es. classificazione atti e supporto al cittadino).
  - Promuove il **riuso**: se un Comune sviluppa un buon sistema di IA (es. per i tributi), questo deve essere messo a disposizione degli altri enti tramite il catalogo dei software di AgID.

---

## 2. Il Garante Privacy: La Tutela dei Diritti

Il Garante interviene quando l'IA "tocca" le persone. Il suo approccio è basato sulla prevenzione della discriminazione e sulla trasparenza.

- **Provvedimenti su Algoritmi e Lavoro Pubblico (Gennaio 2025):**
  - Il Garante ha ribadito che l'uso di algoritmi per valutare le performance dei dipendenti o per decidere turnazioni deve essere **trasparente**. Il dipendente deve poter conoscere i parametri usati dalla macchina.
- **Decalogo sull'IA Generativa (2024/2025):** \* A seguito del caso ChatGPT, il Garante ha emanato prescrizioni rigide: chi usa IA deve garantire che i dati non vengano usati per "auto-addestramento" senza consenso (molto importante per Kibernetes: i dati dei cittadini non devono mai uscire dal perimetro sicuro dell'ente).
- **Provvedimenti contro il "Web Scraping" (Ottobre 2025):**
  - Ha imposto restrizioni tecniche per impedire che software di IA "peschino" dati dai siti della PA per profilare i cittadini senza base giuridica.

---

### Tabella Comparativa delle Competenze (da distribuire in aula)

Caratteristica	AgID (Efficienza Tecnica)	Garante Privacy (Diritto della Persona)
<b>Obiettivo</b>	Modernizzare la PA e standardizzare i sistemi.	Proteggere i dati e prevenire discriminazioni.

---

Caratteristica	AgID (Efficienza Tecnica)	Garante Privacy (Diritto della Persona)
<b>Focus Principale</b>	Sicurezza informatica, interoperabilità, AI Act.	Rispetto del GDPR, trasparenza, non-profilazione.
<b>Cosa controlla?</b>	Che il software sia a norma tecnica e non sprechi risorse.	Che il trattamento dei dati sia lecito e non opaco.
<b>Documento chiave</b>	Linee Guida IA nella PA (2025).	DPIA (Valutazione Impatto) e Decalogo IA.
<b>Autorità di riferimento</b>	Designata dall'AI Act (Nazionale).	Autorità di controllo ex Art. 51 GDPR.

### Un consiglio per il tuo commento finale in aula:

Fai notare agli allievi che mentre AgID dice "**come**" implementare l'IA (es. quali standard usare), il Garante dice "**se**" e "**a quali condizioni**" si può fare (es. rispettando la dignità del cittadino).

**Punto chiave per Kibernetes:** Un progetto IA di successo nella PA deve superare entrambi gli "esami": quello tecnico di AgID e quello etico/giuridico del Garante. Se manca uno dei due, il progetto è a rischio sanzione o annullamento.

**Ti servirebbe un esempio di "check-list" che gli impiegati possano usare per capire se un nuovo software che stanno acquistando rispetta entrambi questi mondi?**

Hai detto

SI GRAZIE vorrei la check list

### Gemini ha detto

Questa checklist è pensata come uno strumento operativo "da scrivania" per gli impiegati. Serve a capire se un progetto o un software che utilizza l'IA è conforme sia all'**AI Act** (normativa tecnica e di prodotto) sia al **GDPR** (protezione dei dati), integrando le disposizioni della **L. 132/2025**.

Puoi distribuirla come esercitazione pratica: chiedi loro di analizzare un software che usano abitualmente alla luce di questi punti.

## Checklist di Conformità IA per la Pubblica Amministrazione

### 1. Inquadramento e Rischio (AI Act & L. 132/2025)

- **Classificazione:** Abbiamo identificato se il sistema è ad "Alto Rischio" (es. selezione personale, sussidi, istruzione, accesso a servizi pubblici)?

- **Divieti:** Il sistema evita pratiche vietate (es. punteggio sociale, riconoscimento delle emozioni sul posto di lavoro, identificazione biometrica non autorizzata)?
- **Finalità Pubblica:** È chiaro l'interesse pubblico perseguito? (Art. 1 L. 132/2025).

## 2. Protezione Dati e Profilazione (GDPR)

- **DPIA (Valutazione Impatto):** È stata aggiornata la DPIA includendo i rischi specifici dell'algoritmo (opacità, errori, bias)?
- **Base Giuridica:** Esiste una norma di legge o regolamento che autorizza questo specifico trattamento automatizzato?
- **Profilazione:** Se il sistema profila i cittadini, è stata prevista una procedura per gestire il diritto di opposizione?

## 3. Trasparenza e Relazione col Cittadino (Art. 15 L. 132/2025)

- **Etichettatura:** Le comunicazioni prodotte dall'IA contengono la dicitura "*Documento assistito da sistemi di IA*"?
- **Informativa:** Il cittadino è informato che sta interagendo con un'IA o che una decisione lo riguarda in quanto frutto di elaborazione algoritmica?
- **Spiegabilità:** Se il cittadino chiede "perché ho avuto questo punteggio?", l'operatore è in grado di estrarre dal sistema la logica della decisione?

## 4. Supervisione Umana (Human-in-the-loop)

- **Validazione Finale:** Esiste un passaggio obbligatorio in cui un funzionario umano approva, firma o convalida l'output dell'IA? (Art. 14 L. 132/2025).
- **Capacità di Intervento:** Il dipendente ha la formazione e il potere tecnico di ignorare o correggere il suggerimento della macchina?
- **Log e Audit:** Il sistema registra chi ha validato la decisione e se sono state apportate modifiche umane all'output?

## 5. Qualità e Sicurezza (AgID & ACN)

- **Data Quality:** I dati di addestramento o di input sono esatti, aggiornati e privi di pregiudizi (bias) statistici?
- **Conformità Tecnica:** Il fornitore (es. Kibernetes) ha fornito la documentazione tecnica richiesta dalle Linee Guida AgID 2025?
- **Cybersicurezza:** Il sistema è protetto contro tentativi di manipolazione dei dati o degli algoritmi?

---

### Suggerimento per la lezione

Fai notare che l'ispezione del Garante per il **primo semestre 2026** si concentrerà proprio sull'**IA in ambito scolastico e nei servizi pubblici**. Spiega che la checklist non è "burocrazia", ma è la prova dell'**Accountability** (Responsabilità): in caso di controllo, l'ente deve dimostrare di aver seguito questi step.

---

### **Materiale extra per te:**

**Idea per chiudere la docenza:** > "Cari colleghi, la Legge 132/2025 ci dice che l'IA è un collega instancabile ma un po' distratto: fa il lavoro grosso, ma siamo noi a dover controllare che non faccia errori di valutazione. La vostra firma è ciò che trasforma un calcolo matematico in un atto amministrativo legittimo."

**C'è qualche altro punto della legge o un caso d'uso specifico di Palermo che vorresti che io analizzassi per arricchire la tua traccia?**

Hai detto

quali sono gli articoli della legge 132/2025 che impongono obblighi a imprese e liberi professionisti?

### **Gemini ha detto**

La **Legge 23 settembre 2025, n. 132** introduce obblighi specifici che impattano direttamente il settore privato, con un occhio di riguardo alla tutela del rapporto fiduciario tra professionista e cliente e alla dignità del lavoratore.

Ecco l'analisi degli articoli che impongono i principali obblighi a imprese e liberi professionisti:

---

## IV Obblighi per imprese e liberi professionisti

### 1. Liberi Professionisti: Il Pilastro della Trasparenza

Il legislatore ha dedicato un'attenzione particolare alle "professioni intellettuali" (avvocati, commercialisti, ingegneri, medici, ecc.), consapevole che l'IA potrebbe alterare il rapporto di fiducia.

- **Art. 13 - Obbligo di Informativa e Prevalenza Umana:**
    - **Informativa al Cliente:** Il professionista ha l'obbligo di comunicare al cliente l'uso di sistemi di IA nella prestazione. Tale comunicazione deve essere resa con linguaggio **chiaro, semplice ed esaustivo**.
    - **Natura Strumentale:** L'IA può essere utilizzata solo per attività **strumentali e di supporto**. La legge impone la **prevalenza del lavoro intellettuale** dell'uomo: il professionista non può delegare interamente la prestazione alla macchina.
  - **Art. 24 - Obbligo Formativo:**
    - Viene demandato agli Ordini Professionali l'obbligo di integrare nei piani formativi un **monte ore minimo** dedicato all'uso delle tecnologie digitali e dell'IA, per garantire che il professionista usi tali strumenti in modo critico e consapevole.
- 

### 2. Imprese e Datori di Lavoro: Gestione e Welfare

Per le imprese, la legge si concentra sull'uso dell'IA nei processi decisionali e nella gestione delle risorse umane, integrando quanto già previsto dall'AI Act e dal GDPR.

- **Art. 10 - IA e Rapporto di Lavoro:**
    - **Principio di Non-Discriminazione:** Le imprese devono garantire che l'uso degli algoritmi non determini effetti discriminatori o pregiudizievoli (per sesso, età, etnia, ecc.).
    - **Miglioramento delle Condizioni:** L'IA deve essere impiegata per migliorare la qualità delle prestazioni e la produttività, ma sempre nel rispetto della **dignità del lavoratore** e della sua integrità psico-fisica.
  - **Obblighi Informativi (In combinato con l'AI Act):**
    - Le imprese devono informare preventivamente i lavoratori e le rappresentanze sindacali se intendono utilizzare sistemi di IA per: **selezione/assunzione, valutazione delle performance, assegnazione mansioni o cessazione del rapporto**.
- 

### 3. Disposizioni comuni e tutela della Proprietà Intellettuale

- **Art. 4 - Tutela dei Minori:** Le imprese che offrono servizi di IA devono garantire che per i minori di 14 anni il consenso sia espresso dai genitori. Per i minori tra 14 e 18 anni, l'informativa deve essere "facilmente accessibile e comprensibile".

- **Art. 26 - Diritto d'Autore:** Introduce obblighi per le imprese che addestrano modelli di IA, sanzionando penalmente la riproduzione o l'estrazione di dati e testi (data scraping) effettuata in violazione delle norme sul diritto d'autore.

Soggetto	Articolo	Obbligo Principale
Professionista	Art. 13	Informare il cliente dell'uso di IA e mantenere la "prevalenza" umana.
Impresa (Employer)	Art. 10	Garantire trasparenza e non-discriminazione negli algoritmi HR.
Professionista	Art. 24	Formazione continua obbligatoria sulle nuove tecnologie.
Aziende Software	Art. 4 / 26	Protezione minori e rispetto del copyright nell'addestramento.

Ecco un modello di **Informativa per Professionisti** (Avvocati, Commercialisti, Ingegneri, Architetti, Consulenti del Lavoro) redatto secondo i requisiti dell'**Art. 13 della Legge 132/2025**.

Questo documento può essere integrato nella lettera d'incarico o nel preventivo professionale.

---

## Modello di Informativa sull'uso dell'Intelligenza Artificiale

(Ai sensi dell'Art. 13 L. 132/2025 e degli Artt. 13-14 del GDPR)

### 1. Utilizzo di sistemi di Intelligenza Artificiale

Il sottoscritto/Lo Studio comunica che, nell'espletamento dell'incarico professionale conferito, potrà avvalersi del supporto di sistemi di Intelligenza Artificiale (IA) per finalità meramente strumentali.

### 2. Finalità e Natura dello strumento

L'uso dell'IA è finalizzato esclusivamente all'ottimizzazione della prestazione professionale (es. analisi preliminare di grandi moli di documenti, ricerca giurisprudenziale/normativa, traduzioni tecniche, bozze di calcolo).

- **Strumentalità:** Il sistema di IA agisce come supporto tecnico e non sostituisce in alcun caso il giudizio professionale dell'essere umano.
- **Controllo:** Ogni output generato dall'IA è sottoposto a rigorosa verifica, revisione e validazione da parte del professionista responsabile.

### 3. Prevalenza del lavoro intellettuale (Art. 13, comma 2)

In conformità alla legge, la prestazione professionale rimane fondata sulla **prevalenza dell'apporto intellettuale umano**. La decisione finale, la strategia adottata e la firma di ogni atto o documento restano di esclusiva responsabilità del professionista, che ne garantisce la coerenza e la correttezza rispetto al caso concreto.

#### **4. Riservatezza e Sicurezza dei Dati (GDPR)**

I dati personali e le informazioni riservate fornite dal Cliente:

- Vengono trattati tramite sistemi di IA "chiusi" o aziendali che garantiscono la non diffusione delle informazioni verso l'esterno.
- **Non** vengono utilizzati per l'addestramento (training) di modelli di IA di terze parti (es. versioni pubbliche di ChatGPT), a meno di esplicito consenso.
- Sono protetti da misure di sicurezza conformi alle linee guida ACN (Agenzia per la Cybersicurezza Nazionale).

#### **5. Diritti del Cliente**

Il Cliente ha il diritto di richiedere in qualsiasi momento chiarimenti sulla specifica logica utilizzata dall'IA nel supporto alla sua pratica e di opporsi all'uso di tali strumenti qualora ritenga che possano pregiudicare il rapporto fiduciario, previa valutazione della fattibilità tecnica della prestazione.

Questa tipologia di modello serve a evitare due grandi rischi legali:

1. **L'annullabilità del contratto:** Se il cliente scopre che un parere è stato scritto da un'IA senza essere stato avvertito, potrebbe contestare la parcella per "mancanza di prestazione intellettuale".
2. **La violazione del segreto professionale:** Inserire dati sensibili dei clienti in IA pubbliche (che "imparano" dai dati inseriti) è una violazione del segreto professionale e del GDPR. L'informativa serve anche a rassicurare il cliente che lo studio usa strumenti sicuri.