Intelligenza Artificiale nella PA: innovazione, Cybersecurity e Data Governance. Principi, strumenti e applicazioni dell'IA per la sicurezza informatica, la gestione dei dati e l'innovazione dei processi pubblici

L'intelligenza artificiale è diventato il riferimento di molti progetti di innovazione nella Pubblica Amministrazione. Il corso ha l'obiettivo di coniugare gli aspetti amministrativi e procedimentali della PA con le potenzialità dei sistemi dotati di IA, continuamente e velocemente in evoluzione. Ciò anche in relazione al Regolamento UE 2024/1689 entrato in vigore il primo agosto scorso ed alla Legge italiana sull'Intelligenza Artificiale.

Questo nei vari settori amministrativi ove operano algoritmi valutativi, chatbot di approfondimento tematico, sistemi redazionali di atti, sistemi di selezione del personale.

Obiettivo è quello di acquisire nozioni sull'IA applicata all'attività amministrativa con l'evidenza delle influenze e dei limiti posti dall'ordinamento, anche in relazione a temi come la tutela della riservatezza.

Vengono esaminate perciò le nuove Linee Guida su IA nella PA, attualmente in consultazione ai fini della loro prossima emanazione, che individuano gli effetti dei principi fondanti dell'IA nei contesti amministrativi a maggior impatto per l'organizzazione ed i cittadini.

Con la Parte Applicativa si analizzano le realizzazioni concrete dell'IA ne processi e nelle attività più strategiche della PA

I PARTE

PROCEDIMENTI AMMINISTRATIVI ED IA

STRUTTURA GENERALE

MODULO 1 – FONDAMENTI DI IA E CONTESTO NORMATIVO

Lezione interattiva + dibattito

CONTENUTI:

1.1 Cos'è l'intelligenza artificiale

Definizioni: dall'IA "debole" all'IA generativa
Machine Learning, Deep Learning, LLM (Large Language Models)
Sistemi deterministici vs. probabilistici
Bias, allucinazioni, limiti attuali

1.2 Il quadro normativo europeo e italiano

Regolamento UE 2024/1689 (AI Act): principi, obblighi, categorie di rischio
Legge italiana 23.09.2025, n. 132: delega al Governo, competenze, governance
Linee Guida AgID su IA nella PA (in emanazione): principi fondanti
Rapporto con GDPR, D.Lgs. 165/2001, D.Lgs. 267/2000

1.3 Principi fondanti per la PA

Trasparenza e accountability
Liceità e non discriminazione
Adeguatezza e proporzionalità
Supervisione umana obbligatoria
Responsabilità e imputabilità

1.4 Discrezionalità amministrativa e automatismo algoritmico

Il limite costituzionale della discrezionalità amministrativa (art. 3, 97 Cost.)
Quando l'IA può supportare e quando NO
Decisioni interamente automatizzate: divieti e eccezioni
Il principio del "human in the loop"

MODULO 2 – IA E DISCREZIONALITÀ AMMINISTRATIVA. GOVERNANCE E RESPONSABILITÀ

Lezione + esercitazioni

DESTINATARI PRIORITARI: Dirigenti, funzionari di staff, DPO, referenti IA

CONTENUTI:

2.1 Discrezionalità tecnica vs. discrezionalità amministrativa

Quando l'IA può assistere: valutazione di fatti complessi
Quando l'IA non può decidere: scelte di indirizzo politico-amministrativo
Esempi concreti: priorità assegnazione servizi (IA può aiutare) vs. definizione obiettivi (no)
Giurisprudenza amministrativa sui sistemi automatizzati

2.2 Governance dell'IA nella PA locale

Ruoli e responsabilità:

Responsabile dell'IA (referente tecnico e normativo)
RTd (responsabile della trasparenza algoritmica)
DPO (aspetti privacy e GDPR)
UPD (se coinvolto in procedimenti sensibili)
Dirigente (responsabile della legalità della decisione)

Documenti essenziali:

Register of high-risk AI systems
DPIA (Data Protection Impact Assessment)
Valutazione di impatto algoritmica
Istruzioni operative di utilizzo

2.3 Trasparenza algoritmica e accountability

Obbligo di comunicare l'uso di sistemi automatizzati (art. 22 GDPR, AI Act)
Motivazione della decisione: quando e come comunicare
Diritto all'accesso e all'algoritmo: limiti e bilanciamento
Diritto di contestazione e ricorso
Documentazione e tracciabilità: cosa registrare, come, per quanto tempo

2.4 Rischi, responsabilità civile e amministrativa

Chi risponde se l'algoritmo sbaglia: ente, dirigente, fornitore?
Responsabilità contrattuale vs. extracontrattuale

Negligenza nell'implementazione e nel controllo: rischi per il dirigente

Assicurazioni e tutela legale

Casi giurisprudenziali

MODULO 3 – IA NEGLI APPALTI E NELLA GESTIONE GARE

Lezione + esercitazioni pratiche

DESTINATARI PRIORITARI: Responsabili di gara, funzionari appalti, RUP, RTD

CONTENUTI:

3.1 Applicazioni attuali dell'IA negli appalti

Gestione amministrativa delle gare:

Screening preliminare candidati (requisiti formali, SOA, antimafia)

Classificazione automatica di ditte per settori/competenze

Estrazione dati da documenti (certificati, visure, fatturati)

Analisi delle offerte:

Anomalia detection: individuazione offerte sospette e "fuori mercato"

Estrazione e normalizzazione prezzi e condizioni

Segmentazione per complessità contrattuale

Support alla valutazione: confronto con benchmark storici

Prevenzione della corruzione:

Identificazione di possibili conflitti di interesse

Monitoraggio SOP (Soglia di Osservazione Particolare) - Anac

Rilevazione di pattern di collusione

3.2 Vincoli normativi e cautele

Codice dei Contratti Pubblici (D.Lgs. 36/2023): compatibilità con trasparenza

AI Act: applicabilità ai sistemi di ranking/scoring

Principi di gara: parità di trattamento, trasparenza, non discriminazione

Verifica della robustezza dell'algoritmo prima del deployment:

Test su dataset storico

Validazione dei bias

Documentazione di training e accuracy

3.3 Aspetti procedimentali critici

Comunicazione ai partecipanti: quando, come, con quale dettaglio

Contestabilità: diritto all'accesso all'algoritmo (limiti legittimi: segreti commerciali)

Responsabilità: la decisione resta sempre umana (dirigente/RUP)

Tracciabilità: cosa documentare nei fascicoli di gara

3.4 Casi d'uso pratico: dalla teoria alla realizzazione

Fasi di implementazione:

Analisi delle esigenze e perimetro d'uso

Scelta dello strumento (proprietary vs. open source)

Training e testing

Pilot su un subset di gare

Rollout con monitoraggio

MODULO 4 – IA NEL RECLUTAMENTO E NEI CONCORSI

Lezione + laboratorio interattivo

DESTINATARI PRIORITARI: Responsabili HR, dirigenti risorse umane, commissari concorsi, funzionari selezione

CONTENUTI:

4.1 Applicazioni dell'IA nel reclutamento pubblico

Screening preliminare:

Verifica requisiti (titoli di studio, certificazioni, lingue)

Valutazione CV: estrazione automatica dati, scoring

Identificazione potenziali candidati idonei

Valutazione delle soft skills:

Sentiment analysis di lettera motivazionale

Linguistic analysis (coerenza, chiarezza)

Predictive scoring: probabilità di successo nel ruolo

⚠ CAUTELE: alto rischio discriminatorio

Colloqui e prove:

Preselezionati da algoritmo vs. selezione casuale

Valutazione video-interviste (facial recognition, tone analysis) — molto critico

Supporto alla commissione: sintesi automatica delle risposte

Matching candidato-profilo:

Ranking finale per posizione desiderata

Segmentazione per specializzazioni

4.2 Vincoli normativi stringenti (CCNL, legge, principi giuridici)

CCNL Funzioni Locali 2022-2024: principi di selettività, merito, trasparenza

D.Lgs. 165/2001: criteri di valutazione non discriminatori

GDPR e AI Act: profilazione, discriminazione, opacità algoritmica

Art. 97 Cost.: imparzialità della PA

Principio di parità di trattamento: come garantirlo?

Divieti assoluti:

Inferenza di attributi protetti (origine etnica, orientamento sessuale, disabilità rilevante)

Valutazione basata su pattern storici discriminatori

Esclusione automatica senza revisione umana

4.3 Responsabilità in caso di errore o contestazione

Chi risponde se candidato idoneo è scartato dall'algoritmo?

Ricorso giurisdizionale: cosa deve provare il ricorrente?

Documentazione della commissione: cosa registrare?

Diritto di accesso all'algoritmo e ai dati di training

4.4 Buone pratiche internazionali e casi studio

Amministrazioni che hanno implementato IA in concorsi (benchmarking)

Cosa ha funzionato, cosa no

Lezioni apprese

MODULO 5 – IA E COMUNICAZIONE PUBBLICA. CHATBOT E ASSISTENTI VIRTUALI

Lezione + laboratorio + casi studio

DESTINATARI PRIORITARI: URP, responsabili comunicazione, gestori servizi online, chatbot manager

CONTENUTI:

5.1 Applicazioni: chatbot e assistenti virtuali nella PA

Chatbot informativi:

Risposta a domande frequenti (FAQ) con linguaggio naturale
Navigazione servizi: "Dove richiedo la carta d'identità?"
Info su procedimenti: stato della pratica, tempi, documenti
Supporto su diritti: agevolazioni, permessi, sussidi

Assistenti conversazionali avanzati:

Raccolta di informazioni complesse (multistep)
Precompilazione di form
Triage di richieste verso uffici competenti
Supporto multilingue

5.2 Benefici e rischi

☑ **Benefici:**

Disponibilità 24/7
Riduzione carico URP
Velocizzazione risposte
Accessibilità migliorata

⚠ **Rischi critici:**

Allucinazioni: l'IA fornisce informazioni inventate (es. leggi che non esistono, procedure errate)
Disinformazione accidentale: risposta plausibile ma falsa
Mancanza di contesto: non sa che il cittadino è in una situazione particolare
Liability: la PA è responsabile di ciò che il chatbot comunica?
Privacy: conservazione di conversazioni; profilazione implicita

5.3 Vincoli normativi

Trasparenza: obbligo di comunicare che è un bot, non una persona
Accuratezza: responsabilità PA per informazioni fornite
Accessibilità: WCAG 2.1 per persone con disabilità
Privacy e GDPR: base giuridica del trattamento dati conversazionali
Prevenzione abusi: chatbot non deve essere usato per raccogliere dati sensibili senza consenso esplicito

5.4 Governance e controllo di qualità

Ciclo di vita: design → training → testing → deployment → monitoring → aggiornamento
Dataset di training: qualità, bias, rappresentatività
Feedback loop: cittadini segnalano errori → team corregge → bot impara
Metriche: accuratezza, satisfaction, drop-off rate, escalation rate

5.5 Buone pratiche

Sempre offrire escalation umana ("Parla con un operatore")
Disclaimer chiaro su limiti del bot

Informativa privacy sulla conservazione chat

FAQ di fallback per argomenti non gestiti

Aggiornamento periodico basato su feedback

MODULO 6 – WORKSHOP INTEGRATIVO: GOVERNANCE, ORGANIZZAZIONE, ROADMAP

Workshop collaborativo + piano d'azione

DESTINATARI PRIORITARI: Referenti IA, DPO, RTd, dirigenti di staff, direttore generale

CONTENUTI:

6.1 Organizzazione della governance dell'IA in ente

Ruoli e responsabilità (ripresa sintetica):

Responsabile IA (coordinamento organizzativo)

RTd (trasparenza algoritmica, comunicazioni)

DPO (privacy, GDPR)

UPD (se coinvolto)

Dirigente/Direttore Generale (accountabilty finale)

Team multidisciplinare: chi manca nella vostra organizzazione?

6.2 Risk management e compliance

Matrice di rischio semplificata per IA

Audit periodico (auto-assessment)

Compliance checklist

Documentazione essenziale da mantenere

6.3 Roadmap di implementazione per un ente locale

Fase 1 (Mesi 1-3): Assessment

Inventario: dove siamo già usi di IA? (es. software gestionali con automazione)

Gap analysis: compliance normativa

Identificazione quick wins (priorità basse)

Fase 2 (Mesi 4-6): Pilot su un'area a basso rischio

Scegliere un caso d'uso concreto (es. chatbot per info generiche)

Strutturare governance e documentazione

Testare processo di control

Raccogliere feedback

Fase 3 (Mesi 7-12): Scaling graduale

Estensione ad altri use case

Integrazione con processi

Monitoraggio e aggiustamenti

Formazione continua del personale

6.4 Formazione interna continuativa

Percorsi di apprendimento per profili:

Livello base (tutti): cosa è l'IA, principi, responsabilità personale

Livello intermedio (operatori): uso pratico, prompt engineering, controllo di qualità

Livello avanzato (referenti, dirigenti): governance, valutazione algoritmi, scenario planning

Metodologie: lezioni, workshop, peer learning, casi studio

II PARTE

IA, Cyber Security e Data Governance per la PA

Modulo 1: Fondamenti di Intelligenza Artificiale e il Valore dei Dati Pubblici

Obiettivo: Demistificare l'IA distinguendo realtà da fantascienza, spiegando come gli algoritmi apprendono e perché i dati sono un bene comune essenziale.

Contenuti:

- Dall'algoritmo deterministico (regole fisse) al Machine Learning e all'IA Generativa: comprendere il riconoscimento di pattern (*pattern recognition*).
- Il principio *"Garbage In, Garbage Out"*: perché la qualità del dato determina la bontà del servizio pubblico.
- Il ciclo di vita del dato pubblico: acquisizione, conservazione, fruizione e dismissione.

Applicazioni nella PA:

- Categorizzazione automatica del protocollo e instradamento rapido delle pratiche amministrative tra uffici comunali o ministeriali.
- Trascrizione e sintesi automatizzata dei verbali di Consigli e Giunte comunali.

Modulo 2: Data Governance, Qualità e Trasparenza Amministrativa

Obiettivo: Trasmettere le basi organizzative per governare il patrimonio informativo pubblico evitando silos e discriminazioni algoritmiche.

Contenuti:

- Ruoli e responsabilità sui dati (*Data Owner*, *Data Custodian*, responsabile di procedimento).
- Catalogazione, metadati e tracciabilità (*Data Lineage*): sapere sempre da dove provengono i dati e chi vi ha accesso.
- Distorsioni cognitive e algoritmiche (*Bias*): come prevenire disparità di trattamento nei servizi al cittadino.

Applicazioni nella PA:

- Interoperabilità delle banche dati pubbliche (es. PDND - Piattaforma Digitale Nazionale Dati) per attuare il principio *"Once Only"*.
- Bonifica e standardizzazione degli indirizzi anagrafici e catastali per tributi locali equi e trasparenti.

Modulo 3: Privacy, Etica e Quadro Normativo (EU AI Act e GDPR)

Obiettivo: Fornire una bussola legale per orientarsi tra conformità, diritti fondamentali e doveri del funzionario pubblico.

Contenuti:

- Principio di proporzionalità e minimizzazione dei dati applicato ai modelli intelligenti (GDPR).
- L'**EU AI Act**: sistema a piramide del rischio (rischio inaccettabile, alto rischio, rischio minimo/trasparenza) e obblighi per i soggetti pubblici.
- Principio di riserva dell'intervento umano (*Human-in-the-loop*): la decisione amministrativa finale resta sempre una responsabilità umana.

Applicazioni nella PA:

- Analisi preventiva di conformità (DPIA e AI Assessment) prima di acquistare o implementare un software algoritmico nella scuola, nella sanità locale o nei servizi sociali.

- Linee guida sul divieto di pratiche vietate (es. social scoring o riconoscimento biometrico indiscriminato nei luoghi pubblici).

Modulo 4: Cyber Security – Minacce Moderne Potenziate dall'IA

Obiettivo: Comprendere come i criminali informatici utilizzano l'IA per attaccare il perimetro pubblico e colpire il personale.

Contenuti:

- I pilastri della sicurezza informatica: Riservatezza, Integrità, Disponibilità (CIA).
- L'ingegneria sociale di nuova generazione: email di phishing iper-personalizzate, deepfake audio/video per truffe d'identità (*CEO/Mayor Fraud*).
- Il fenomeno della *Shadow IA*: pericoli dell'inserimento di atti confidenziali, bozze di delibere o dati di cittadini all'interno di chatbot pubblici gratuiti.

Applicazioni nella PA:

- Simulazione e riconoscimento di comunicazioni ingannevoli inviate ai funzionari dell'Ufficio Gare/Appalti o Ragioneria per distrarre pagamenti o carpire credenziali di rete.
- Redazione di una *Acceptable Use Policy* (Policy d'Uso Consentito) interna per l'utilizzo responsabile di strumenti di produttività basati su IA.

Modulo 5: Cyber Difesa con l'IA e Resilienza Operativa

Obiettivo: Illustrare come le tecnologie intelligenti proteggono le reti della PA e come gestire l'imprevisto operativo.

Contenuti:

- L'IA per la difesa: individuazione precoce delle anomalie di traffico, rilevamento di accessi anomali e contrasto ai ransomware.
- Vulnerabilità tipiche dei sistemi IA: manipolazione dei prompt (*Prompt Injection*) e avvelenamento delle basi di conoscenza (*Data Poisoning*).
- Continuità operativa e gestione degli incidenti: la catena di segnalazione in caso di violazione dati (*Data Breach*).

Applicazioni nella PA:

- Sistemi di protezione perimetrale automatizzati a difesa di siti istituzionali e portali di pagamento pagoPA contro attacchi DDoS.
- Procedure operative di notifica e coordinamento con l'ACN (Agenzia per la Cybersicurezza Nazionale) e il Garante Privacy.

Modulo 6: Workshop Operativo, Strategia e Gestione del Cambiamento

Obiettivo: Mettere a terra i concetti appresi attraverso simulazioni di scenari reali di appalto, implementazione e risposta a crisi.

Contenuti:

- Il ciclo di vita di un progetto IA nella PA: dal capitolato tecnico all'audit periodico.
- La gestione della trasparenza: motivazione dell'atto amministrativo supportato da algoritmi.
- Esercitazione pratica a gruppi: simulazione di redazione di requisiti di sicurezza e governance per un bando pubblico.

Applicazioni nella PA (Casi pratici d'aula):

- *Caso A:* Progettazione di un assistente virtuale per i Servizi Sociali (riservatezza, assenza di bias nei criteri di assegnazione aiuti, sicurezza dei dati sanitari/anagrafici).
- *Caso B:* Gestione di una crisi causata da una risposta fuorviante (*allucinazione*) rilasciata al pubblico da un bot informativo comunale su una scadenza tributaria.