Governance dell'IA nella PA

Avv.ta Adriana Augenti

Se un algoritmo nega un sussidio a una famiglia sbagliata, di chi è la colpa?

Il fatto che non esista una risposta immediata è già un problema.

Mappa della lezione

01

L'algoritmo è un atto amministrativo

02

La PA come deployer ad alto rischio

03

DPIA, AIIA, FRIA — non sono la stessa cosa

04

La responsabilità che scotta (L. 1/2026)

05

Quando l'IA pubblica sbaglia — e cosa ne ricaviamo

BLOCCO 1

L'algoritmo è un atto amministrativo

La domanda rimasta senza risposta

> *Se un algoritmo nega un sussidio a una famiglia sbagliata, di chi è la colpa?*

Il funzionario

Ha usato l'algoritmo senza capirlo.

Il dirigente

Ha adottato il sistema senza valutarlo.

L'ente

Non ha effettuato le valutazioni d'impatto richieste dalla legge.

Il Consiglio di Stato ha risposto a questa domanda nel 2019. Con l'AI Act, ignorarla è diventato più costoso.

Le due sentenze: fatti di cronaca

Cons. Stato n. 2270/2019 e n. 8472/2019

"La regola tecnica dell'algoritmo ha piena valenza giuridica e amministrativa."

Cosa significa

L'algoritmo non è uno strumento istruttorio neutro. È, a tutti gli effetti, una **decisione amministrativa robotizzata**.

L'algoritmo non è il soggetto della decisione. È il **contenuto** della decisione.

Il soggetto siete voi.

Principio 1 — La scatola nera

Spiegabilità / XAI — Explainable AI

Lo scenario

Un cittadino impugna il diniego di un contributo comunale. Il suo avvocato chiede: *"Su quale base logica il sistema ha deciso?"* Il funzionario risponde: *"Non lo so, lo decide l'algoritmo."*

L'atto è impugnabile. Anzi, è già illegittimo.

Il principio

La spiegabilità è la traduzione digitale dell'**obbligo di motivazione** che esiste nel diritto amministrativo da secoli. Se l'iter logico della macchina non è comprensibile, l'atto che ne deriva non è motivabile.

La giurisprudenza si aggiorna: le sentenze del 2025

Due pronunce che ampliano il perimetro

Cons. Stato n. 4929/2025 — Il caso ARGEA/SIAN

ACCESSO AGLI ATTI

Due cittadine richiedono accesso al fascicolo di un coerede per verificare la legittimità di contributi agricoli gestiti tramite il Sistema Informativo Agricolo Nazionale (SIAN). L'amministrazione oppone diniego per "complessità algoritmica" e onerosità dell'intervento del gestore del software.

Il Consiglio di Stato annulla il diniego.

> *"Le difficoltà tecniche derivanti dall'uso dell'IA non possono costituire un ostacolo al diritto di accesso. La PA non può invocare la gestione esternalizzata dei sistemi per sottrarsi ai doveri di trasparenza."*

Principio violato: Spiegabilità / XAI

Cons. Stato n. 8092/2025 — L'IA negli appalti

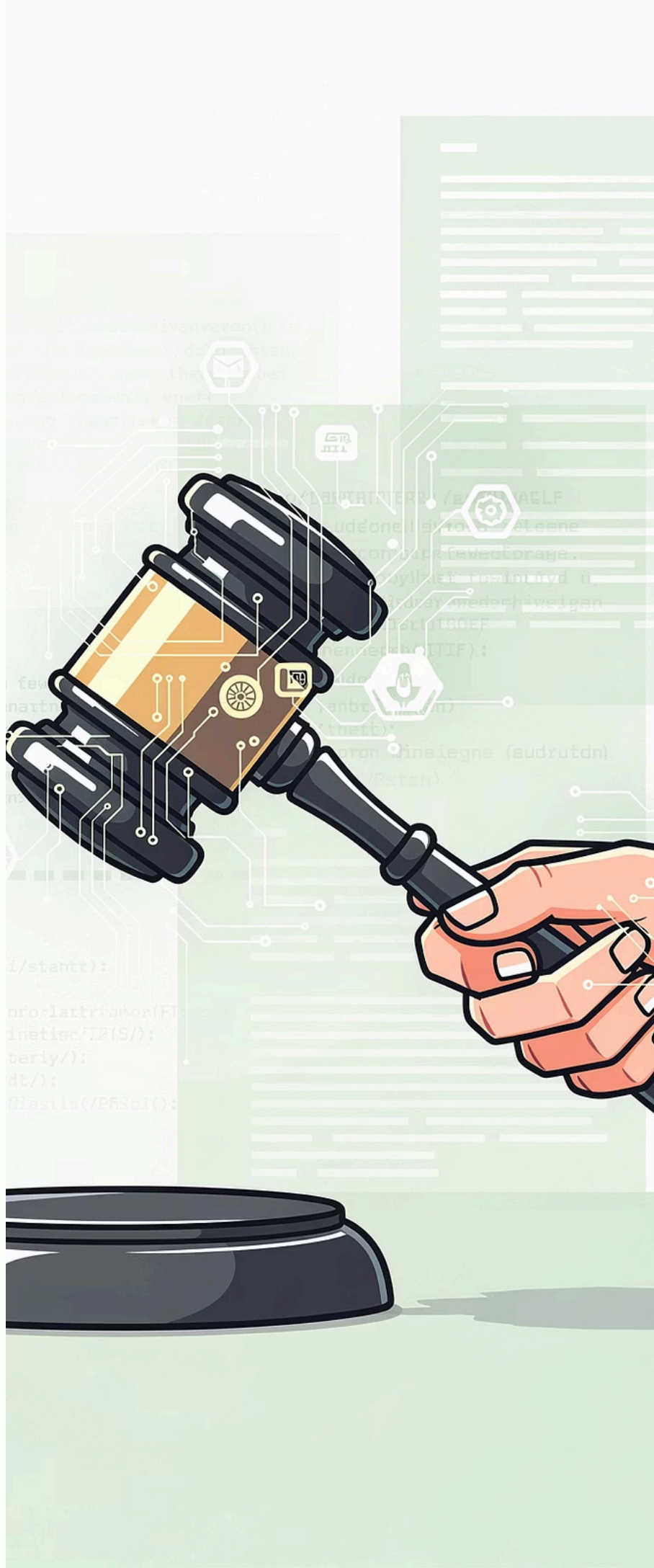
GARE PUBBLICHE

Un operatore economico usa ChatGPT per redigere proposte tecniche in una gara d'appalto. Il concorrente contesta la legittimità dell'offerta.

Il Consiglio di Stato conferma la legittimità.

- L'uso dell'IA non rende l'offerta incongrua, purché supportata da un piano di implementazione operativa chiaro e verificabile
- La valutazione della congruità rientra nella discrezionalità tecnica della stazione appaltante
- Chi contesta l'uso dell'IA altrui deve fornire prove oggettive, non opinioni soggettive

Implicazione: le stazioni appaltanti devono aggiornare i criteri di valutazione per pesare l'efficacia delle tecnologie algoritmiche



Art. 30 D.Lgs. 36/2023 — Lo statuto dell'IA negli appalti

Il Codice dei Contratti Pubblici anticipa l'AI Act

Cosa dice l'art. 30

Le stazioni appaltanti devono automatizzare le proprie attività ricorrendo, ove possibile, a soluzioni tecnologiche – incluse l'intelligenza artificiale e le tecnologie di registri distribuiti.

(D.Lgs. 31 marzo 2023, n. 36, art. 30, comma 1)

- **Disponibilità del codice sorgente:** obbligo di rendere disponibile il codice sorgente, la documentazione e ogni elemento utile a comprendere le logiche di funzionamento del sistema (comma 2)
- **Clausole di assistenza nei bandi:** gli atti di indizione delle gare devono contenere clausole che garantiscano prestazioni di assistenza e manutenzione per tutta la durata del contratto
- **Sicurezza by design:** misure di sicurezza adeguate devono essere integrate fin dalla progettazione del sistema

Il collegamento con la giurisprudenza

Cons. Stato 8092/2025 — ChatGPT negli appalti

L'uso dell'IA nelle offerte tecniche è legittimo se supportato da un piano operativo concreto. L'art. 30 impone ora alle stazioni appaltanti di dotarsi di criteri oggettivi per valutare l'efficacia delle tecnologie algoritmiche nelle offerte.

Cons. Stato 4929/2025 — Accesso agli atti SIAN

L'obbligo di disponibilità del codice sorgente e della documentazione (art. 30, co. 2, lett. a) rende inaccettabile il diniego di accesso per "complessità algoritmica": la PA deve poter spiegare il sistema che ha acquistato.

Il principio unificante

Chi acquista un sistema IA senza pretendere trasparenza sul suo funzionamento viola già l'art. 30. La spiegabilità non è solo un principio etico: è un obbligo contrattuale.

> La stazione appaltante che non sa come funziona il sistema che ha comprato non può governarlo. E se non può governarlo, non può rispondere delle sue decisioni.

Principio 2 — La delega totale

Non esclusività — Human-in-the-loop

Lo scenario

Il sistema suggerisce di revocare un'autorizzazione commerciale. Il funzionario firma senza esaminare il fascicolo. In giudizio emerge che il sistema aveva elaborato dati obsoleti.

Chi ha sbagliato?

Il principio

L'intervento umano nella decisione amministrativa è **insopprimibile**. Una decisione che produce effetti giuridici su un cittadino deve avere, in ultima istanza, un essere umano che se ne assume la responsabilità.

Attenzione: il controllo umano deve essere *significativo*. Apporre una firma dopo che l'algoritmo ha già deciso tutto non è controllo – è ratifica acritica. Ed è esattamente il comportamento che la Corte dei Conti sta imparando a sanzionare.

Principio 3 — Il pregiudizio invisibile

Non discriminazione — Bias algoritmico

Lo scenario

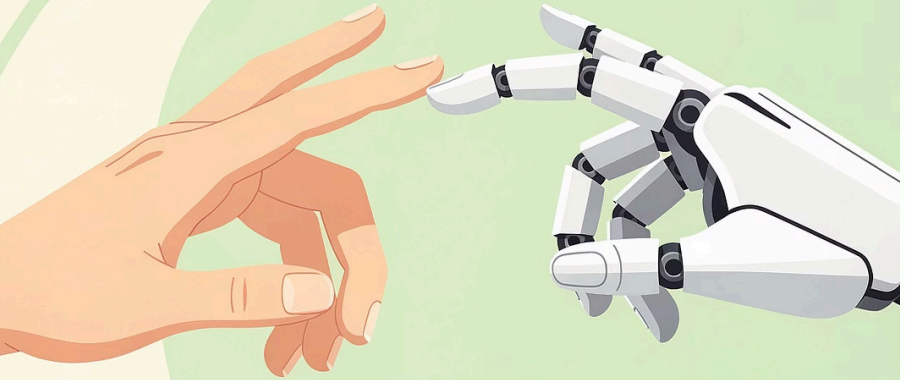
Un algoritmo di selezione del personale pubblico, addestrato su dati storici, scarta sistematicamente i profili femminili per le posizioni dirigenziali. Nessuno se n'è accorto perché *"è il sistema che decide"*.

> Il sistema ha imparato dai dati. I dati rispecchiavano un passato discriminatorio. Il futuro ha riprodotto il passato – in modo automatico, scalabile e apparentemente neutro.

Il principio

Il bias algoritmico nasce dai dati di addestramento. I dati storici della PA italiana non sono un modello di parità. Un algoritmo addestrato su quella storia tenderà a perpetuarla – in modo invisibile, rapido e su scala molto più larga di qualsiasi singolo funzionario.

Il Presidente Stanzione (Garante Privacy) ha parlato esplicitamente di necessità di **"parità algoritmica"**.



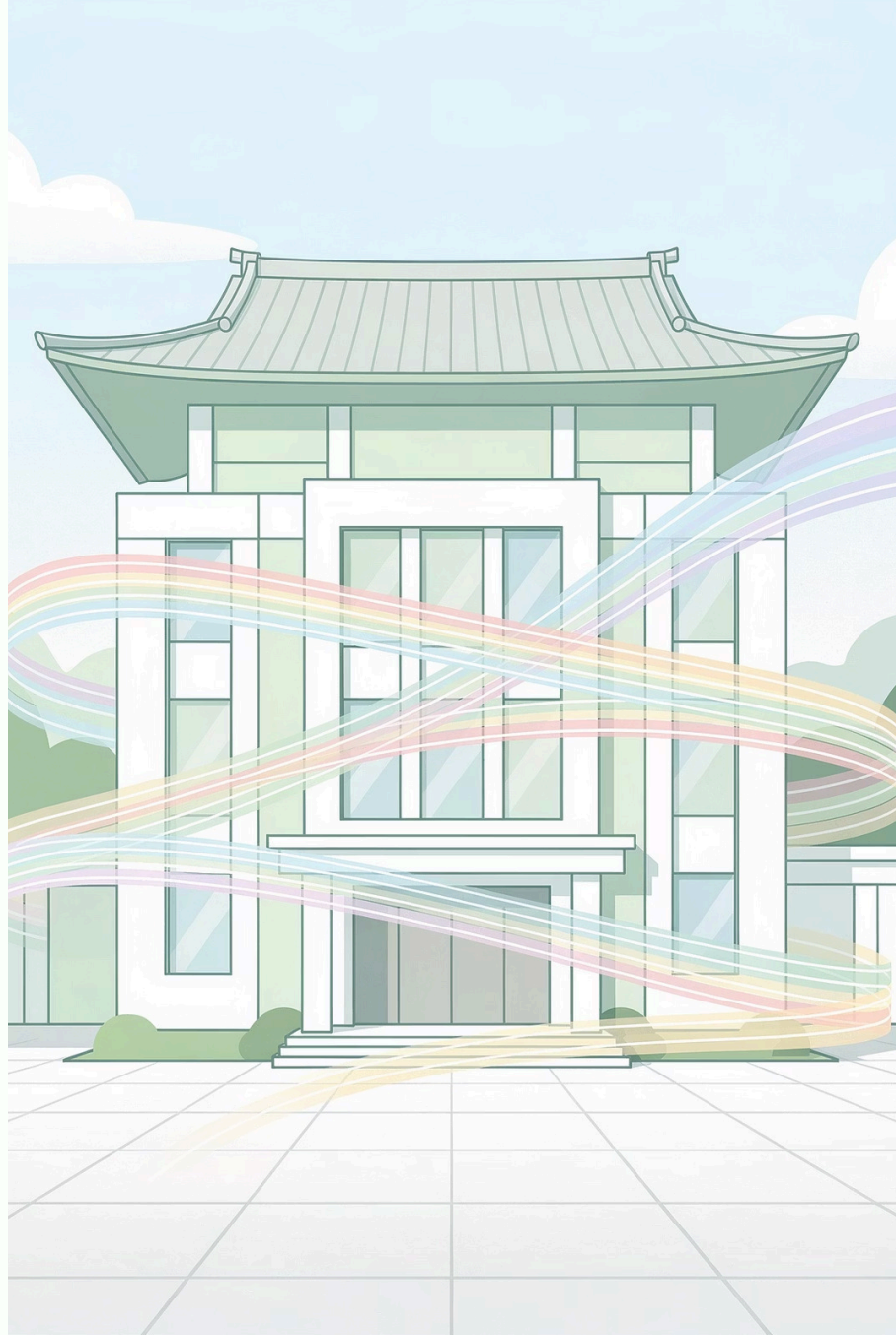
L'algoritmo non decide al posto tuo. Decide con te. E la responsabilità è tua.

Torna utile quando parliamo di polizze assicurative obbligatorie.

BLOCCO 2

La PA come deployer ad alto rischio

Essere deployer non è una posizione comoda. È una posizione esposta.



BLOCCO 2

La Legge 132/2025: il recepimento italiano

Legge 23 settembre 2025, n. 132

Recepimento italiano dell'AI Act

- Art. 1 – Principio di autodeterminazione umana: l'IA non può sostituire la decisione finale del funzionario
- Art. 3 – Qualità e rappresentatività dei dati: obbligo di verifica del dataset prima del deploy
- Definizione di "sistema IA": ampia, include chatbot, scoring, analisi predittiva, riconoscimento facciale

Cosa cambia per la PA

Censimento obbligatorio

Ogni tecnologia in uso va classificata: anche strumenti non nati come IA possono ricadere nel regime di conformità

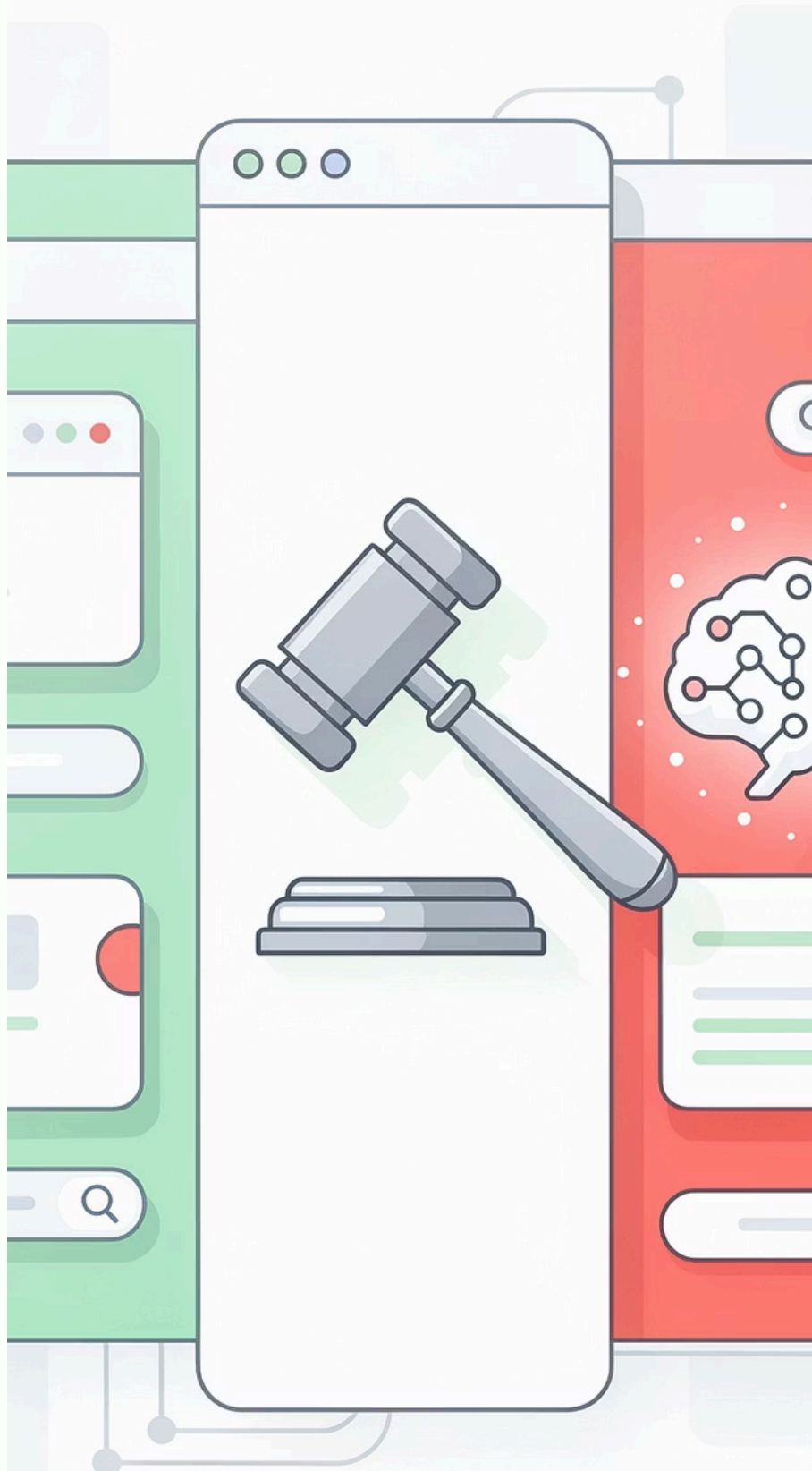
Autodeterminazione umana

L'IA amplifica la capacità del funzionario, non la sostituisce. La decisione finale resta sempre in capo a una persona fisica

Dataset sotto esame

I dati di addestramento devono essere rappresentativi della popolazione e privi di distorsioni statisticamente rilevabili

> L'ampiezza della definizione impone a ogni Amministrazione un censimento sistematico di tutte le tecnologie in uso.



Chi è il deployer? Una distinzione che cambia tutto

PROVIDER	DEPLOYER
Chi progetta e sviluppa il sistema IA	Chi lo usa su persone reali
Google, Microsoft, startup specializzate	Il tuo Comune, la tua Provincia, il tuo Ministero
Risponde della **costruzione**	Risponde dell'**uso**

"Il software lo ha fatto una ditta esterna, se sbaglia è colpa loro." – Sbagliato. Sono due piani di responsabilità distinti e non si escludono a vicenda.

I sistemi ad alto rischio: dove opera la PA

L'AI Act classifica i sistemi IA per livello di rischio. La PA opera quasi esclusivamente nella fascia alta – per l'**asimmetria di potere** tra amministrazione e cittadino.

Sussidi e welfare

Gestione del personale

Amministrazione della giustizia

Servizi essenziali ai cittadini

Controllo del territorio

Quando sbaglia un algoritmo pubblico che gestisce un sussidio o una graduatoria, il cittadino non ha alternative – e il danno è spesso irreversibile.

I tre obblighi del deployer

1

Sorveglianza umana attiva

Il funzionario deve comprendere cosa ha fatto il sistema, identificare anomalie e – se necessario – disattendere l'output. Se non è in grado di farlo, il problema è dell'ente che ha adottato il sistema in quelle condizioni.

2

Conservazione dei log per 6 mesi

Non è un dettaglio tecnico. È la traccia che permette – in caso di ricorso, indagine o ispezione del Garante – di ricostruire cosa ha deciso il sistema e perché. Log assenti o incompleti: violazione già configurata.

3

Trasparenza verso il cittadino

Il cittadino che subisce una decisione automatizzata ha il diritto di saperlo – in modo chiaro, comprensibile, accessibile. Non sepolto nelle note a piè di pagina di un provvedimento di quaranta pagine.

L'analogia del direttore dei lavori

> Il direttore dei lavori firma il collaudo di un'opera che non ha costruito mattone per mattone. Se l'opera crolla, risponde lui – non il muratore che ha posato il cemento.

Voi siete il direttore dei lavori

Il software è l'opera

Il cittadino è chi ci abita

Il collaudo porta la vostra firma

La responsabilità non aspetta che la formazione sia completa.

Il Registro degli Algoritmi: non un adempimento, un'ancora

La vostra amministrazione sa quali sistemi IA sta usando?

Il Registro degli Algoritmi (Strategia italiana per l'IA 2024-2026) è il documento che dimostra che l'ente **sapeva cosa stava usando**, perché, con quali garanzie e con quale supervisione umana.

- → Finalità e base giuridica del sistema
- → Fornitore e specifiche tecniche
- → Categorie di dati trattati
- → Esiti delle valutazioni d'impatto
- → Misure di supervisione umana

Se non riuscite a rispondere a nessuna di queste domande per i sistemi che usate quotidianamente, avete già un problema. Non domani – adesso.

AI Governance Board e Regulatory Sandbox

AI Regulatory Sandbox

Spazi di sperimentazione controllata gestiti in collaborazione con AgID e ACN. Consentono di testare sistemi ad alto rischio in condizioni di sicurezza giuridica, prima del lancio definitivo del servizio. Le autorità forniscono orientamenti interpretativi e supporto tecnico.

Per le PA che vogliono innovare senza esporsi a rischi legali ingestibili.

AI Governance Board / AI Ethics Officer

Composizione interdisciplinare

Giuristi, esperti di etica, data scientist, responsabili organizzativi. Non un ufficio burocratico: un presidio etico.

Funzioni operative

Supervisiona il Registro degli Algoritmi, coordina FRIA e AIIA, funge da interlocutore istituzionale con AgID e ACN.

Perché è necessario

La scelta tecnologica non può essere lasciata ai soli tecnici informatici. Le implicazioni etiche e giuridiche richiedono competenze trasversali.

> Non si tratta di nuovi uffici burocratici: si tratta di presidi etici il cui valore è garantire che la scelta tecnologica non venga lasciata ai soli tecnici informatici.

TrasparenzAI e Sicurezza by Design

L'IA che controlla l'IA – e i rischi che nessuno vede

TrasparenzAI — ANAC (settembre 2025)

Piattaforma open source realizzata con il supporto del CNR. Analizza automaticamente le sezioni "Amministrazione Trasparente" di oltre 23.600 siti pubblici italiani.

23.600

siti pubblici monitorati automaticamente

< 20h

per completare un'analisi che richiederebbe anni di lavoro umano

Non solo finalità sanzionatorie: fornisce alle PA un check di conformità immediato. La trasparenza da adempimento formale a fattore abilitante.

Sicurezza by Design — ACN

L'IA introduce vulnerabilità nuove che la PA deve presidiare fin dalla progettazione.

Avvelenamento dei dati (Data Poisoning)

Attacchi che manipolano i dati di addestramento per alterare gli output del sistema. Obbligo: backup offline dei dataset critici.

Red Teaming

Valutazioni di sicurezza invasive obbligatorie prima del rilascio di sistemi ad alto impatto. Simulazione di scenari di attacco reali.

Supply Chain & Debito Tecnico

La scelta del modello IA deve basarsi su un'analisi delle minacce dell'intera catena di approvvigionamento. Evitare interventi veloci che compromettano la resilienza futura.

> La sicurezza non si aggiunge dopo: si progetta dentro. Un sistema IA non sicuro non è mai conforme, anche se tecnicamente funzionante.

Il cambio di prospettiva

Prima

> *"Il software lo ha fatto una ditta esterna."*

Dopo

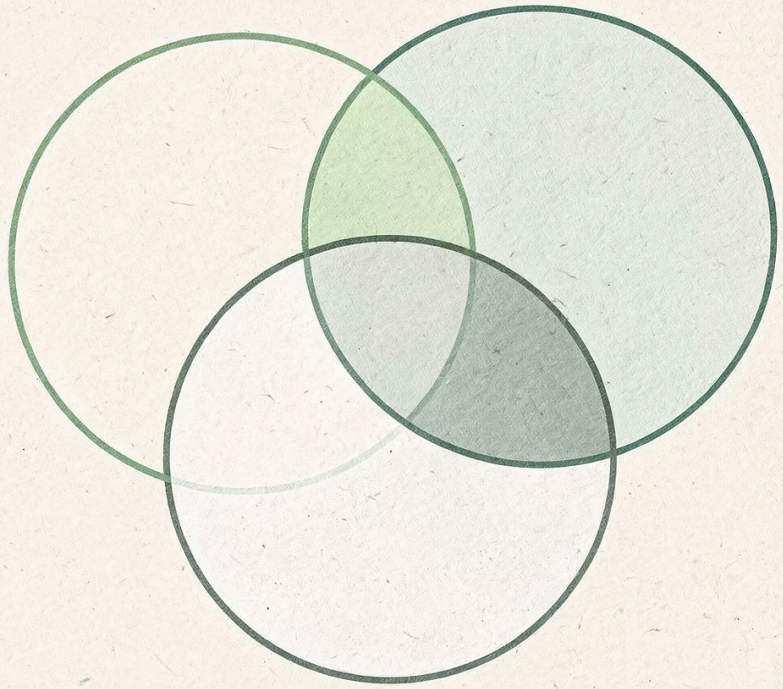
"L'uso del software è responsabilità mia."

Gli strumenti per tutelarsi esistono – ma vanno usati prima, non dopo.

BLOCCO 3

Il trittico delle valutazioni d'impatto

Non basta la DPIA. Non è mai bastata. E adesso è anche obbligatorio dirlo.



Tre domande, tre strumenti

🔒 DPIA

Il sistema protegge i dati personali dei cittadini?

⚙️ AIIA

Il sistema è robusto, sicuro e organizzativamente sostenibile?

⚖️ FRIA

Il sistema è giusto?

Molti enti pensano che rispondere alla prima sia sufficiente. Non lo è. Con la Legge 132/2025 che recepisce l'AI Act nell'ordinamento italiano, ignorare le altre due ha conseguenze molto concrete.

DPIA — Il territorio familiare

Data Protection Impact Assessment

Base normativa: **GDPR art. 35**

Domanda: *Il sistema protegge i dati personali?*

Quando: prima del trattamento, se ad alto rischio

Chi: il titolare del trattamento (l'ente)

Output: registro, misure correttive, eventuale consultazione preventiva del Garante

Cosa valuta — e cosa non valuta

La DPIA valuta il rischio che un trattamento di dati personali produca sui diritti e le libertà delle persone fisiche. È obbligatoria ogni volta che si usano dati su larga scala, si monitorano sistematicamente le persone, o si trattano categorie particolari di dati.

La DPIA è **necessaria ma non sufficiente**. Protegge il dato – non valuta se il sistema che usa quel dato è robusto, equo o sicuro in senso più ampio.

Fare la DPIA e archiviarla non è governance. È un adempimento. La governance è quello che ci costruisci sopra.

AIIA — Il territorio intermedio

AI Impact Assessment

Base normativa: **Linee Guida AgID (2025)**

Domanda: *Il sistema è robusto, sicuro e organizzativamente sostenibile?*

Quando: prima dell'adozione del sistema

Chi: l'amministrazione che adotta

Output: valutazione tecnica, organizzativa, di sicurezza

Il livello intermedio

L'AIIA valuta la robustezza tecnologica del sistema, la sua sicurezza informatica, la sua sostenibilità organizzativa. Si chiede: questo sistema funziona come deve? L'ente ha le competenze per gestirlo? I processi interni reggono l'integrazione?

Più profondo della DPIA (non guarda solo i dati, ma l'intero sistema). Meno profondo della FRIA (non si interroga sulle conseguenze etiche e sui diritti fondamentali).

In molti enti italiani, questa valutazione non viene fatta perché nessuno sa che esiste.

FRIA — Il territorio nuovo e scomodo

Fundamental Rights Impact Assessment

Base normativa: **AI Act art. 27**

Domanda: *Il sistema è giusto?*

Quando: prima della messa in servizio – obbligatoria per tutti i sistemi ad alto rischio

Chi: il deployer (l'ente pubblico)

Output: analisi multidisciplinare + **sintesi pubblica obbligatoria**

Notifica: all'autorità di vigilanza

La grande novità dell'AI Act

Non si chiede se il sistema funziona (AIIA). Non si chiede se protegge i dati (DPIA). Si chiede se il sistema è **giusto**: se rispetta i diritti fondamentali, se non discrimina, se non comprime libertà, se non danneggia i gruppi vulnerabili.

La FRIA non è un documento interno. Richiede una sintesi pubblica – i cittadini devono poter sapere quali misure di salvaguardia l'ente ha adottato. Non è una scelta. È un obbligo.

Le cinque fasi della FRIA

1

1. Pianificazione

Team multidisciplinare, coinvolgimento dei portatori di interesse

2

2. Valutazione

Analisi su categorie vulnerabili, simulazione di scenari anche impropri

3

3. Mitigazione

Definizione dei controlli, struttura della supervisione umana

4

4. Reporting

Pubblicazione della sintesi, notifica all'autorità di vigilanza

5

5. Monitoraggio

Revisione periodica, gestione degli incidenti, aggiornamento

Una valutazione fatta una volta e mai aggiornata non è una valutazione – è un documento storico.

La tabella comparativa

	DPIA	AIIA	FRIA
Domanda	I dati sono protetti?	Il sistema funziona bene?	Il sistema è giusto?
Base normativa	GDPR art. 35	Linee Guida AgID	AI Act art. 27
Oggetto	Trattamento dati	Sistema IA	Diritti fondamentali
Obbligatoria per la PA	Sì, se alto rischio dati	Sì, per adozione IA	Sì, per sistemi ad alto rischio
Pubblica	No	No	**Sì — sintesi obbligatoria**

L'unica con obbligo di pubblicità è la FRIA – quella che incide più direttamente sui diritti dei cittadini, e che il legislatore ha voluto rendere verificabile dall'esterno.

L'errore che fanno quasi tutti

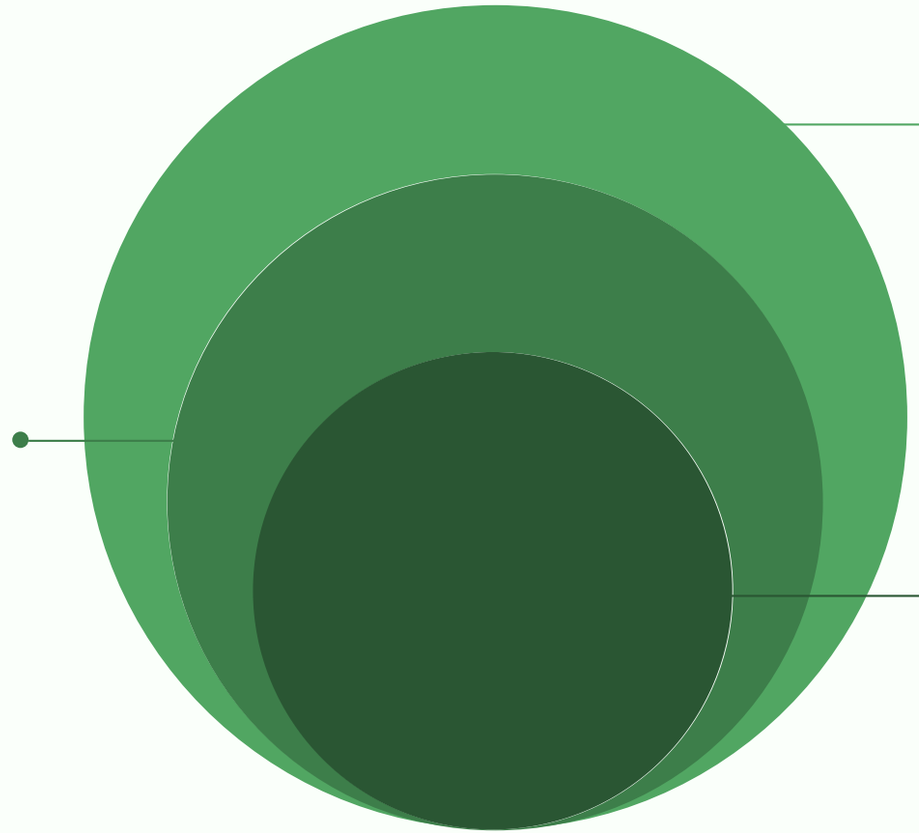
> *"Abbiamo fatto la DPIA. Siamo a posto."*

No.

La DPIA è necessaria ma non sufficiente. Non valuta la robustezza del sistema (AIIA). Non valuta l'impatto sui diritti fondamentali (FRIA). Un ente che ha fatto solo la DPIA ha soddisfatto **un terzo** dei propri obblighi valutativi.

La conformità non è uno stato binario. È un percorso – ma va iniziato con una mappa onesta della situazione attuale.

I tre cerchi: una gerarchia di profondità



DPIA: Il dato

Gestione, minimizzazione e sicurezza dei dati

AIIA: Il sistema

Valutazione progettuale e controlli tecnici

FRIA: La persona

Protezione e diritti dell'individuo

Ogni livello include il precedente, ma nessuno lo sostituisce. Servono tutti e tre – in quest'ordine, **prima** della messa in servizio del sistema, non dopo che qualcosa è andato storto.

BLOCCO 4

La responsabilità che scotta

Legge 7 gennaio 2026, n. 1

L'evoluzione della paura

1

Anni '90

"Paura della firma" – tendenza a non decidere per non rischiare la Corte dei Conti

2

Anni 2010

"Paura della digitalizzazione" – resistenza all'innovazione per timore di errori

3

2026

"Paura dell'algoritmo" – non adottare nulla, o delegare tutto alla macchina

Entrambe le strategie – non adottare nulla e delegare tutto – sono sbagliate. Entrambe espongono. La Legge 1/2026 ha cercato un equilibrio.

La novità strutturale: l'obbligo assicurativo

> **Chiunque gestisca risorse pubbliche deve stipulare una polizza assicurativa a copertura dei danni patrimoniali cagionati per colpa grave.**
>
> *(L. 7 gennaio 2026, n. 1)*

Prima implicazione

Le compagnie assicurative inizieranno a fare domande sulla governance dell'IA negli enti che assicurano. Chi non ha documentazione potrebbe trovarsi con premi più alti o coperture più strette.

Seconda implicazione

Avere una polizza non significa essere al riparo. Il danno viene coperto – ma il giudizio contabile e la responsabilità reputazionale restano.

Cos'è la colpa grave nel contesto algoritmico

> *La colpa grave si configura in caso di violazione manifesta delle norme, travisamento dei fatti o negazione di evidenze risultanti dagli atti.* (L. 1/2026)

Scenario A

Il funzionario firma un atto basato sull'output algoritmico senza verificare che i dati di input siano corretti e aggiornati.

Scenario B

Il dirigente adotta un sistema IA ignorando bias discriminatori già segnalati in letteratura o da precedenti casi analoghi.

Scenario C

L'ente usa un sistema ad alto rischio senza aver condotto le valutazioni d'impatto obbligatorie (DPIA, AIIA, FRIA).

La colpa grave non richiede dolo. Richiede di aver ignorato quello che era ragionevolmente conoscibile e ragionevolmente prevedibile.

I limiti del risarcimento

30%

del danno accertato

Tetto massimo al risarcimento patrimoniale

2x

la retribuzione lorda annua

Limite alternativo – si applica il minore dei due importi

Il tetto è una rete di sicurezza. Non elimina il giudizio contabile (pubblico, con conseguenze reputazionali), le sanzioni del Garante Privacy, né la responsabilità disciplinare interna. La rete non impedisce di cadere – ammortizza l'atterraggio.

L'automation bias come elemento costitutivo della colpa

Automation bias

La tendenza a fidarsi eccessivamente dell'output di un sistema automatizzato, riducendo o eliminando il giudizio critico personale.

Non è una debolezza caratteriale. È un meccanismo cognitivo documentato.

Nel contesto della responsabilità amministrativa

Il meccanismo è amplificato dal carico di lavoro e dalla cultura della copertura burocratica – per cui avere "il sistema che ha detto così" sembra una protezione. Non lo è.

La Legge 132/2025 è esplicita: il controllo umano deve essere **significativo**. Il funzionario che firma comunque su un sistema opaco **non è tutelato**. Sta firmando in bianco.

🔗 Il collegamento con l'esperimento della collega Paglieri

«Il rischio non è che un modello possa sbagliare, è che possa essere persuaso.» Se la macchina cede all'istruzione e ignora i fatti, e il funzionario si fida ciecamente di quella macchina 'persuasa' apponendo la sua firma – i due problemi si sommano. L'automation bias è il corollario umano della vulnerabilità algoritmica: insieme, producono la colpa grave e il danno erariale.

Domande dalla platea

Due questioni che la norma non ha ancora risolto del tutto

❓ DOMANDA 1

«NotebookLM è un problema? Uso lo stesso account Google di lavoro...»

Sì, è un problema – ed è l'esempio perfetto di quello che i tecnici chiamano Shadow AI: l'uso di strumenti IA non autorizzati, non censiti e non contrattualizzati dall'Ente, spesso in buona fede.

Deployer inconsapevole

Caricando atti amministrativi su un LLM non contrattualizzato per la PA, l'Ente diventa deployer di un sistema IA che non ha mai autorizzato, valutato né inserito nel Registro degli Algoritmi.

Dati pubblici fuori controllo

I documenti caricati escono dal perimetro di sicurezza dell'Ente. Non importa che si usi l'account di lavoro: il dato è trattato da un sistema terzo senza base giuridica, senza DPIA, senza informativa al cittadino.

La responsabilità è personale

Il funzionario che usa Shadow AI non è tutelato dalla struttura. Se il trattamento è illecito, risponde lui – non l'Ente, non Google.

⚠ Regola pratica: se il sistema non è nel Registro degli Algoritmi dell'Ente, non usarlo per dati amministrativi. Mai.

❓ DOMANDA 2

«Dobbiamo informare i cittadini anche se usiamo l'IA integrata nei browser?»

La domanda è precisa e la risposta onesta è: il quadro normativo non ha ancora fornito indicazioni operative definitive su questo caso specifico.

L'IA integrata nei browser (Copilot in Edge, AI Overview in Chrome, ecc.) opera in modo trasparente per l'utente ma invisibile per il cittadino che interagisce con la PA. Se un funzionario usa questi strumenti per elaborare una pratica che riguarda un cittadino, si pone il problema dell'obbligo di informativa previsto dall'art. 14 della L. 132/2025 e dal principio di trasparenza dell'AI Act.

Che la risposta non sia ancora definitiva non significa che il problema non esista. Significa che chi pone questa domanda oggi è già un passo avanti rispetto alla norma – e che la risposta arriverà presto, probabilmente sotto forma di sanzione.

La connessione che chiude il cerchio

→ **Nessuna FRIA/DPIA/AIIA**

→ violazione manifesta delle norme → **colpa grave**

→ **Automation bias acritico**

→ travisamento dei fatti → **colpa grave**

→ **Sistema opaco adottato senza verifiche**

→ negazione di evidenze → **colpa grave**

Le valutazioni d'impatto non erano adempimenti burocratici – erano la documentazione che vi protegge. Il Registro degli Algoritmi non era un esercizio accademico – era la traccia che dimostra che l'ente sapeva cosa stava usando. Tutto si tiene.

Le sanzioni reali: quando il Garante interviene

Non è teoria. Sono numeri.

Destinatario	Autorità	Anno	Sanzione	Violazione contestata
OpenAI (ChatGPT)	GPDP	2024	15.000.000 €	Mancanza base giuridica per raccolta dati di addestramento, violazione trasparenza, assenza verifica età
Enel Energia	GPDP	2022	26.500.000 €	Telemarketing aggressivo basato su algoritmi di profilazione non autorizzati
Foodinho (Glovo)	GPDP	2021	2.600.000 €	Gestione algoritmica del lavoro senza informativa adeguata ai lavoratori
Deliveroo Italy	GPDP	2021	2.500.000 €	Algoritmo opaco e discriminatorio nel ranking dei rider
ASUFC (Sanità)	GPDP	2022	55.000 €	Algoritmo Covid-19 senza DPIA e senza base legale specifica
INPS	GPDP	2024	50.000 €	Diffusione non autorizzata di dati personali di partecipanti a concorsi

⚠ Le sanzioni irrogate a soggetti privati come OpenAI o Deliveroo costituiscono già oggi, nelle sentenze della Corte dei Conti, un titolo di responsabilità per il funzionario pubblico che abbia omesso le necessarie valutazioni preventive. Il privato paga la multa. Il funzionario risponde anche erarialmente.

BLOCCO 5

Quando l'IA pubblica sbaglia

Quattro casi reali. Quattro lezioni diverse.

> *I principi si dimenticano. Le persone no.*

CASO 1 — La Toeslagenaffaire

Olanda, 2013–2021

26K

famiglie colpite

Accusate ingiustamente di frode nei sussidi per l'assistenza all'infanzia

2021

caduta del governo

Il governo Rutte III si dimette a gennaio 2021

Il sistema algoritmico per il rilevamento delle frodi includeva implicitamente l'origine etnica tra le variabili. Le famiglie con doppia nazionalità venivano segnalate come sospette a tassi sproporzionati. Alcune persero la casa. Alcune si separarono. Alcune svilupparono patologie psichiatriche documentate.

Principio di non discriminazione – violato. Non esclusività – violato. Spiegabilità – violato. Il costo non è stato solo umano. È stato istituzionale.

CASO 2 — Il paradosso di Amsterdam

Smart Check, 2020

Il paradosso

Codice sorgente **pubblico**, totalmente trasparente.

Esito: riproduzione sistematica di bias contro i migranti.

La lezione

Il sistema era addestrato su dati storici che riflettevano pratiche di controllo discriminatorie – i quartieri a maggioranza migrante erano già stati sottoposti a più controlli, quindi i dati mostravano più irregolarità in quelle aree. L'algoritmo ha imparato e amplificato questa correlazione.

La trasparenza tecnica senza governance etica diventa uno strumento di legittimazione dell'ingiustizia. Ai cittadini non basta sapere che il codice è pubblico. Hanno diritto a sapere che il sistema è giusto. Questo è esattamente ciò che la FRIA garantisce.

CASO 3 — Robodebt

Australia, 2016–2019

470K

persone colpite

1.7B

AUD di debiti generati

Una frazione minima era legittima

Il sistema incrociava dati dichiarati con quelli fiscali e generava automaticamente richieste di restituzione – senza verifica manuale, senza istruttoria, senza contraddittorio. Il difetto tecnico: calcolo su redditi medi annui per lavoratori con redditi variabili settimana per settimana. Centinaia di migliaia di persone vulnerabili ricevettero richieste di restituzione di somme non dovute. La Royal Commission (2023) ha accertato che funzionari di alto livello **sapevano** che il sistema produceva debiti illegittimi. Alcune figure sono state rinviate a giudizio penale.

L'algoritmo non era uno strumento di efficienza. Era uno strumento di impunità. Con la Legge 1/2026, questa strategia non funziona più.

CASO 4 — Bias di genere nella selezione del personale pubblico

Italia — in corso

Il meccanismo

Gli algoritmi di selezione vengono addestrati su dati storici. I dati storici della PA italiana mostrano una sistematica sottorappresentazione femminile nei ruoli apicali. L'algoritmo impara che un dirigente di successo ha caratteristiche più frequentemente associate a profili maschili – e penalizza i profili che si discostano dal modello storico.

Le segnalazioni

Il Presidente Stanzione (Garante Privacy) ha parlato esplicitamente di necessità di **"parità algoritmica"**. La Fundamental Rights Agency UE ha documentato come i bias di genere si amplificano nel tempo attraverso feedback loop. La ricerca accademica italiana conferma il fenomeno specifico per la PA.

⚠️ Il meccanismo del feedback loop

L'output del sistema influenza nel tempo i dati di input successivi, amplificando progressivamente le distorsioni iniziali. Un sistema che tende a scartare donne per ruoli dirigenziali ridurrà nel tempo la presenza femminile nei dati storici – giustificando, secondo la logica algoritmica, la prosecuzione e l'intensificazione della discriminazione. Il monitoraggio continuo degli output reali è indispensabile: non sostituibile con la sola valutazione preventiva.

"Apparentemente neutro" è la parte più pericolosa. Quando il bias ha la veste dell'oggettività tecnologica, è molto più difficile da contestare – per chi lo subisce e per chi dovrebbe fermarlo.

Quattro casi, una lezione

Caso	Cosa è andato storto	Principio violato
Olanda	Bias etnico nel welfare	Non discriminazione + Non esclusività
Amsterdam	Trasparenza senza etica	Governance oltre la tecnica
Australia	Opacità usata come scudo	Spiegabilità + Accountability
Italia	Bias storico nel personale	Non discriminazione + FRIA

Quattro contesti diversi, un solo meccanismo: la governance dell'IA è stata trattata come un problema tecnico quando era un problema politico, giuridico ed etico. Quando la governance manca, non paga la macchina. Pagano le persone.

Checklist operativa per l'ente pubblico

12 adempimenti prima di mettere in servizio un sistema IA

- ☐ Registro degli Algoritmi aggiornato con tutti i sistemi in uso
- ☐ Classificazione del livello di rischio AI Act per ogni sistema
- ☐ DPIA effettuata per ogni trattamento di dati personali tramite IA
- ☐ AIIA effettuata per ogni sistema (robustezza tecnica e organizzativa)
- ☐ FRIA effettuata per ogni sistema ad alto rischio (art. 27 AI Act)
- ☐ Nomina dell'AI Ethics Officer o costituzione dell'AI Governance Board
- ☐ Adozione del Codice Etico per l'IA integrato nel Codice di Comportamento
- ☐ Formazione periodica del personale sull'AI Literacy e sull'automation bias
- ☐ Polizza assicurativa dei dirigenti per colpa grave (L. 1/2026)
- ☐ Procedura interna di segnalazione e gestione degli incidenti algoritmici
- ☐ Verifica della qualità e rappresentatività dei dataset utilizzati
- ☐ Meccanismo di ricorso accessibile per i cittadini che subiscono decisioni algoritmiche

La conformità non è un optional. È l'unica vera ancora di salvezza per il dipendente pubblico – e la garanzia democratica per il cittadino.

BLOCCO 6

Comprare IA in modo responsabile: la Community europea

La Community of Practice on Public Procurement of AI — Commissione Europea

Iniziativa della Commissione Europea che riunisce acquirenti pubblici per condividere conoscenze, sviluppare clausole standard e garantire un'acquisizione di sistemi IA affidabile, equa e sicura. Gestisce il portale Public Buyers Community e il Public Sector Tech Watch.

La PA che acquista IA non è solo deployer: è anche acquirente. E l'acquisto è già governance.

900+

casi d'uso IA nel settore pubblico censiti (Public Sector Tech Watch)

24

lingue in cui sono disponibili le MCC-AI

Le MCC-AI: cosa sono e perché contano

Le clausole contrattuali modello per l'acquisto di IA — aggiornate al 5 marzo 2025

Le MCC-AI sono state pubblicate per la prima volta il 29 settembre 2023 e aggiornate il 5 marzo 2025 per allinearsi all'AI Act (in vigore dal 1° agosto 2024). Non sono un documento ufficiale vincolante, ma rappresentano lo standard di riferimento per la compliance nell'acquisto pubblico di IA.

Versione completa

Per sistemi IA ad alto rischio (Allegato III AI Act). Copre trasparenza, gestione del rischio, responsabilità, governance dei dati.

Versione light

Per sistemi IA non ad alto rischio, ma che possono comunque incidere su salute, sicurezza o diritti fondamentali.

Commentary

Guida pratica su come usare, personalizzare e applicare le clausole in concreto. Disponibile in 24 lingue UE.

Le clausole sono progettate per essere allegate ai contratti, non per sostituirli.

Cosa coprono le MCC-AI: le clausole chiave

Trasparenza e Spiegabilità

Documentazione del funzionamento del sistema, dati di addestramento e limitazioni. La PA deve poter spiegare le decisioni algoritmiche ai cittadini.

Gestione del Rischio

Obbligo di valutazione del rischio prima della messa in servizio. Il fornitore deve notificare incidenti gravi e aggiornamenti rilevanti.

Sorveglianza Umana

Misure tecniche per permettere all'operatore umano di intervenire, sospendere o disattivare il sistema in caso di necessità.

Governance dei Dati

Requisiti per la qualità, pertinenza e rappresentatività dei dati di addestramento. Divieto di bias sistematici e ingiustificati.

Responsabilità e Audit

Diritto della PA di effettuare audit o richiederli a terze parti indipendenti. Conservazione dei log di sistema per almeno 6 mesi.

Aggiornamenti e Manutenzione

Obbligo del fornitore di comunicare tempestivamente aggiornamenti sostanziali e di mantenere la conformità del sistema nel tempo.

Un contratto senza clausole IA-specifiche non è un contratto conforme all'AI Act. È un contratto incompleto.

Le MCC-AI nella pratica: cosa fare adesso

Le Model Contract Clauses per l'IA sono la chiave per l'acquisto responsabile. La Strategia Italiana per l'IA 2024-2026 le integra nelle linee guida per il procurement, rendendole uno strumento fondamentale per la PA.

Prima di bandire la gara

- Classificare il sistema IA per livello di rischio (AI Act Allegato III)
- Scegliere la versione MCC-AI appropriata (full o light)
- Integrare le clausole nel capitolato tecnico o nel contratto
- Verificare la compatibilità con il D.Lgs. 36/2023 (art. 30)

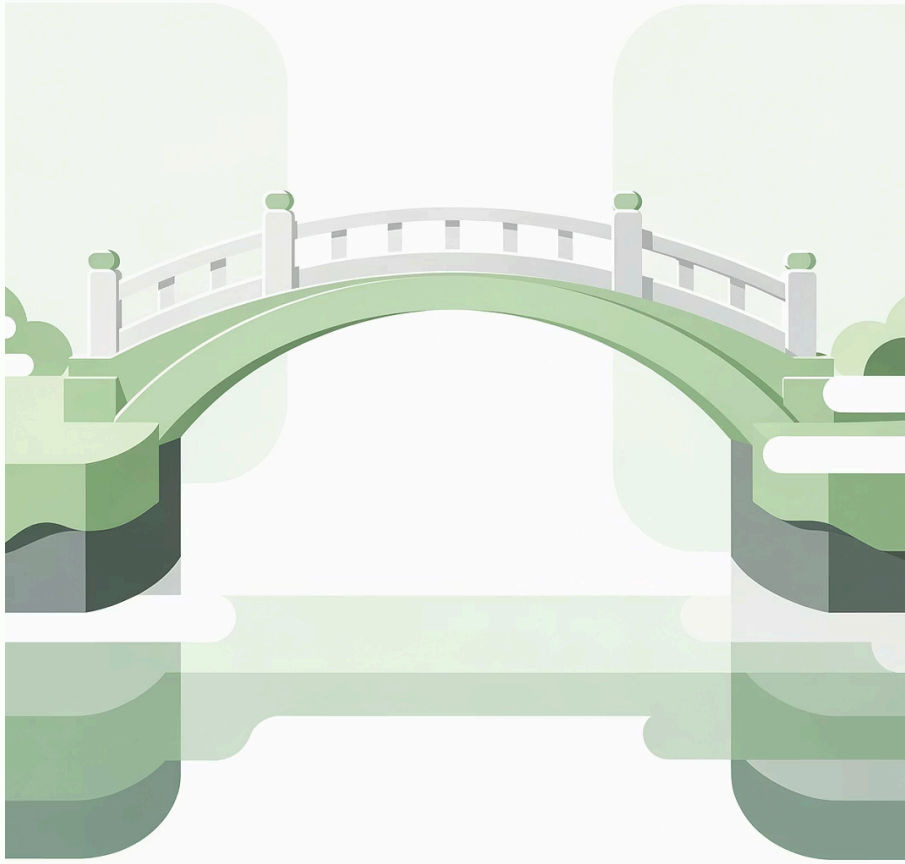
Durante e dopo l'esecuzione

- Richiedere al fornitore la documentazione tecnica prevista dalle clausole
- Attivare i meccanismi di sorveglianza umana previsti contrattualmente
- Conservare i log e la documentazione per eventuali audit
- Aggiornare il Registro degli Algoritmi con i dati del nuovo sistema

Le MCC-AI non sono un optional. Sono la traduzione contrattuale degli obblighi del deployer.

CHIUSURA

Il ponte con l'accessibilità



Accessibilità digitale → Accessibilità algoritmica

Accessibilità digitale (ieri)	Accessibilità algoritmica (oggi)
Garantire che i siti pubblici siano navigabili da tutti, inclusi i non vedenti, gli anziani, le persone con disabilità.	Garantire che le decisioni automatizzate siano comprensibili, contestabili e giuste per tutti i cittadini, inclusi i più vulnerabili.

Il vecchio divide era visibile: il sito non funziona sullo screen reader, il modulo non è compatibile da mobile. Il nuovo divide è **invisibile**: una decisione algoritmicamente generata che nega un sussidio, scarta una candidatura, classifica un profilo come sospetto – e il cittadino non sa perché, non può contestare efficacemente, e spesso non sa nemmeno che è stata una macchina a decidere.

I tre profili di cittadino vulnerabile

Il cittadino digitalmente escluso

Non sa che è stato un algoritmo a decidere. Non ha gli strumenti per contestare.

Fallimento di trasparenza.

Il cittadino discriminato

Sa che qualcosa non va, ma non riesce a dimostrarlo perché il sistema è opaco.

Fallimento di spiegabilità.

Il cittadino informato ma impotente

Sa tutto, capisce tutto, ma l'ente non ha le procedure per rispondere alle sue contestazioni.

Fallimento di governance.

Cosa portarsi a casa: una gerarchia, non una checklist

Base — Sapere

Quali sistemi IA usa la tua amministrazione, su quali procedimenti, su quali categorie di persone. Se non lo sai, non puoi governare nulla.

Livello intermedio — Documentare

Le valutazioni d'impatto non sono carta – sono protezione. Se non sono state fatte, il momento di iniziare non è dopo il prossimo audit. È adesso.

Vertice — Esercitare controllo umano significativo

Non firmare perché il sistema ha detto così. Capire, valutare, e quando necessario dissentire dalla macchina con una motivazione documentata. Questo è il cuore della riserva di umanità che la legge protegge.

"L'etica non è un accessorio. È il sistema operativo."

Governance dell'IA nella PA – Avv.ta Adriana Augenti – CIVITAS 2026