

LA DIFESA CIVICA NELL'ERA DIGITALE

(Guido Giusti)

INDICE

Intelligenza artificiale e Pubblica Amministrazione

Dalla prassi spontanea al governo del sistema

| pag. 2

Superare la crisi della governance

La cornice normativa come infrastruttura di fiducia

| pag. 5

Il ruolo della difesa civica

Nuovi orizzonti nella tutela dei diritti

| pag. 8

Difesa civica e transizione digitale

Proposte e prassi operative

| pag. 12

Conclusioni

pag. 16

1. Intelligenza artificiale e PA

Dalla prassi spontanea al governo del sistema

L'intelligenza artificiale non costituisce più una frontiera tecnologica da esplorare, bensì una condizione di fatto con cui la Pubblica Amministrazione è già chiamata a confrontarsi.

Come accade spesso nei processi di innovazione, il fenomeno ha preceduto la sua regolazione: l'uso dell'IA si è insinuato nel lavoro quotidiano dei pubblici uffici ben prima che l'istituzione ne assumesse piena consapevolezza giuridica e organizzativa.

È proprio in questo scarto tra realtà e pianificazione che si colloca il problema centrale del presente contributo. Non si tratta di stabilire se l'IA debba entrare nella Pubblica Amministrazione, ma se l'Amministrazione sia in grado di governare una tecnologia che già la attraversa, incidendo su tempi, linguaggi, responsabilità e rapporti con i cittadini.

In ogni ufficio pubblico, così come in ogni realtà professionale, strumenti di intelligenza artificiale sono già oggi utilizzati dai dipendenti per redigere testi, sintetizzare documenti, tradurre comunicazioni, organizzare informazioni. Si tratta di un uso spesso individuale, informale, talvolta invisibile all'organizzazione.

Questo comportamento, quando sfocia in un vero e proprio utilizzo indiscriminato, viene definito dagli addetti ai lavori «*shadow AI*», un fenomeno ormai diffusissimo in ogni realtà aziendale e istituzionale. Anche nei casi in cui l'organizzazione vieta (o addirittura blocca) i principali applicativi di IA generativa, come *ChatGPT*, *Gemini*, *Claude* o *Copilot*, i dipendenti aggirano il firewall aziendale utilizzando questi strumenti sui propri dispositivi personali. L'azienda, ovviamente, non è in grado di prevenire né di monitorare tali condotte, con la conseguenza che il problema di sicurezza che si tentava di arginare (in particolare l'esposizione involontaria di dati sensibili in ambienti non autorizzati) si aggrava fino a sfuggire a ogni controllo.

Fonti autorevoli descrivono una crescita molto significativa e non regolamentata dell'uso dell'AI nei contesti lavorativi. Le ricerche evidenziano, infatti, che oltre l'80% dei dipendenti utilizza strumenti di intelligenza artificiale non approvati dall'azienda (UpGuard). Inoltre, più della metà degli utenti di GenAI dichiara di farne uso almeno occasionalmente in modo non dichiarato, e quasi il 50% opera tramite account personali, sottraendosi completamente al controllo aziendale (Netskope). Particolarmente critico è il dato relativo alla sicurezza: il 38% dei lavoratori ammette di condividere dati confidenziali con piattaforme AI senza autorizzazione, mentre il 52% di chi utilizza tali strumenti non ha mai ricevuto alcuna formazione specifica in materia (CybSafe e National Cybersecurity Alliance).

Come già osservava Max Weber, la razionalizzazione amministrativa non procede per decisioni isolate, ma per adattamenti progressivi delle prassi. L'IA si inserisce in questo solco: non come rottura improvvisa, ma come acceleratore silenzioso di modalità operative già esistenti.

Il vero rischio non è l'uso dell'IA in sé, bensì il fatto che tale uso avvenga fuori da ogni cornice di responsabilità istituzionale, in una zona grigia che rende difficile imputare decisioni, errori e conseguenze.

Sotto molti aspetti, la Pubblica Amministrazione è strutturalmente caratterizzata da procedimenti ripetitivi, sequenze codificate e atti standardizzati.

Proprio per questo, l'IA potrebbe rappresentare un'opportunità significativa: non per sostituire il decisore pubblico, ma per alleggerire il lavoro umano dalle componenti meccaniche, consentendo ai funzionari di concentrarsi sulle valutazioni a più alto contenuto giuridico e discrezionale.

Tuttavia, in assenza di una cornice regolatoria chiara e di strumenti istituzionalmente integrati nei sistemi informativi pubblici, si produce un effetto paradossale. Il singolo funzionario, che non ha la possibilità tecnica di interfacciare autonomamente l'IA con i sistemi di protocollo, gestione documentale o workflow procedimentale — normalmente governati da piattaforme centrali soggette a rigorosi vincoli di sicurezza, auditabilità e tracciabilità — finisce per utilizzare l'intelligenza artificiale soprattutto nelle fasi ad alto contenuto cognitivo: redazione di provvedimenti, motivazioni, note istruttorie, sintesi valutative.

In altre parole, proprio le attività che incidono più direttamente sulla sfera giuridica dei cittadini diventano quelle maggiormente esposte a forme di delega informale e non governata, mentre le attività meramente esecutive e procedurali restano rigidamente vincolate ai sistemi ufficiali. Ciò determina una sorta di “asimmetria dell'automazione”: le funzioni meno delicate restano presidiate dall'organizzazione, mentre quelle più sensibili rischiano di essere svolte con strumenti individuali, non tracciati e privi di protocolli di responsabilità.

Questo fenomeno è già stato evidenziato, a livello internazionale, nei documenti dell'OCSE sulla *digital transformation* del settore pubblico e nelle prime linee interpretative dell'AI Act europeo, che sottolineano la necessità di garantire accountability, supervisione umana effettiva e tracciabilità delle decisioni assistite da sistemi di IA, proprio per evitare che l'uso individuale e non istituzionalizzato produca decisioni “opache” sotto il profilo della responsabilità amministrativa.

Ne deriva che il problema non è tanto se i funzionari utilizzano o meno l'intelligenza artificiale — fenomeno ormai inevitabile — quanto piuttosto se tale utilizzo sia incorporato entro infrastrutture organizzative ufficiali, dotate di log di utilizzo, criteri di validazione, policy di controllo e responsabilità chiaramente attribuite. In mancanza di questa integrazione, l'amministrazione rischia di trovarsi nella

situazione singolare in cui l'IA può contribuire, di fatto, alla redazione di un provvedimento amministrativo capace di incidere su diritti, interessi legittimi o posizioni economiche dei cittadini, senza che l'organizzazione disponga degli strumenti per monitorare come tale supporto sia stato utilizzato, con quali dati e secondo quali criteri.

Da qui l'esigenza, sempre più evidente, di passare da un uso spontaneo e individuale dell'IA a una adozione istituzionale governata, capace di ricondurre l'innovazione tecnologica entro i principi tradizionali dell'azione amministrativa — legalità, trasparenza, imputabilità e controllabilità — evitando che l'accelerazione tecnologica produca, paradossalmente, un arretramento delle garanzie.

2. Superare la crisi della governance

La cornice normativa come infrastruttura di fiducia

La regolazione dell'intelligenza artificiale si colloca oggi in un contesto di trasformazione istituzionale caratterizzato da una significativa asincronia: l'innovazione tecnologica evolve con rapidità esponenziale, mentre l'adattamento delle strutture amministrative procede necessariamente secondo i tempi della democrazia e delle garanzie, legati alla produzione normativa e alla riorganizzazione delle competenze.

In questa fase di transizione, le amministrazioni pubbliche operano in un quadro regolatorio in progressivo consolidamento, nel quale strumenti avanzati vengono spesso adottati prima di essere pienamente integrati nei modelli organizzativi e nei sistemi di controllo istituzionali.

Senza una governance esplicita, la tecnologia tende a diffondersi per “inerzia operativa”, sospinta dalle esigenze di smaltimento dell'arretrato e di efficienza quotidiana più che da una strategia consapevole. Il rischio reale non è l'introduzione della tecnologia, quanto la sua adozione silenziosa: l'uso non governato di strumenti che incidono direttamente sull'esercizio dei diritti.

In questo senso, l'intuizione di Lawrence Lessig — *code is law* — assume rinnovata attualità: se non regolata, l'architettura del software finisce per produrre effetti normativi di fatto, dettando le modalità concrete di esercizio del potere amministrativo.

Il problema non riguarda solo gli output (le decisioni), ma anche e soprattutto gli input (i dati). Il principio informatico *garbage in, garbage out* acquisisce qui rilevanza giuridica: dati incompleti, obsoleti o affetti da *bias* storici possono generare decisioni formalmente efficienti ma sostanzialmente illegittime. Ancor più critico è l'uso di piattaforme esterne per il trattamento di dati pubblici, che pone un problema di sovranità informativa: l'ente pubblico rischia di perdere il controllo sul proprio patrimonio conoscitivo strategico, indebolendo la propria funzione di garante del dato.

Un uso non governato favorisce inoltre fenomeni di deresponsabilizzazione decisionale: l'errore viene attribuito alla “macchina”, mentre la decisione appare tecnicamente inevitabile. È il fenomeno del *math-washing*: ammantare di oggettività matematica scelte che restano probabilistiche. Tuttavia, l'ordinamento non conosce una “responsabilità algoritmica”: la responsabilità resta sempre umana e organizzativa. L'IA non è un oracolo di verità, ma uno strumento di calcolo che richiede interpretazione, verifica e, ove necessario, il coraggio del dissenso motivato da parte del funzionario.

Per governare questa complessità, l'ordinamento restituisce oggi un'architettura regolatoria multilivello, articolata su piani complementari.

Il fondamento di questo edificio giuridico è rappresentato dal Regolamento generale sulla protezione dei dati personali (GDPR). Lungi dall'essere un mero strumento burocratico, il Regolamento (UE) 2016/679 ha introdotto nel sistema europeo il principio cardine di accountability, imponendo alle amministrazioni non solo di rispettare le norme, ma di essere in grado di dimostrarlo attraverso una documentazione proattiva delle scelte organizzative. Il cuore della tutela risiede nell'articolo 22, che sancisce il divieto di sottoporre le persone a decisioni basate unicamente sul trattamento automatizzato che producano effetti giuridici o incidano significativamente sulla loro sfera personale, imponendo la presenza di una supervisione umana effettiva e non meramente formale.

La portata di tale divieto è stata scolpita dalla Corte di Giustizia dell'Unione Europea con la sentenza del 7 dicembre 2023 nella causa C-634/21 (Schufa Holding AG). I giudici europei hanno statuito che la generazione automatizzata di un valore di probabilità (come un punteggio di affidabilità o score) costituisce una "decisione basata unicamente sul trattamento automatizzato" ai sensi dell'articolo 22, paragrafo 1, del GDPR, qualora da tale valore dipenda in modo determinante la decisione finale assunta da un terzo. Questo principio assume una rilevanza cruciale per l'azione amministrativa: l'esito elaborato da un algoritmo non può predeterminare in via di fatto le sorti di un procedimento. Il divieto europeo preclude che l'intervento del decisore pubblico si riduca a un mero avallo formale, impedendo che l'algoritmo si trasformi da strumento di supporto istruttorio a decisore occulto.

A questo primo livello di garanzia sui dati si affianca il Regolamento europeo sull'intelligenza artificiale (AI Act). Se il GDPR protegge la persona, il Regolamento (UE) 2024/1689 disciplina lo strumento, adottando un approccio basato sul rischio. Gran parte degli impieghi della Pubblica Amministrazione ricade nella categoria ad "alto rischio": dai sistemi per l'erogazione di servizi essenziali e prestazioni di welfare alle procedure di selezione del personale, fino ai sistemi predittivi utilizzati per valutazioni comportamentali o decisionali.

Per tali ambiti il legislatore europeo impone obblighi operativi stringenti, tra cui la valutazione d'impatto sui diritti fondamentali, standard elevati di governance dei dati e requisiti di trasparenza tecnica (explainability), affinché il funzionamento dei sistemi non resti opaco per chi ne subisce gli effetti.

Discendendo dal piano sovranazionale a quello interno, la Legge italiana sull'intelligenza artificiale (L. 132/2025) assume la funzione di raccordo istituzionale. La normativa nazionale evita di duplicare gli obblighi sostanziali previsti dall'AI Act, concentrandosi sulla definizione della governance interna e sull'individuazione delle autorità competenti — tra cui l'Agenzia per la Cybersicurezza Nazionale (ACN) e l'Agenzia per l'Italia Digitale (AgID) — nonché sui meccanismi di coordinamento tra le amministrazioni. L'obiettivo è prevenire la frammentazione e garantire che la transizione digitale avvenga in modo uniforme e sicuro su tutto il territorio nazionale.

In questa cornice, assume una rilevanza centrale l'articolo 14 della legge, rubricato proprio all'uso dell'intelligenza artificiale nella Pubblica Amministrazione. La norma fissa un perimetro operativo

rigoroso: se da un lato l'IA è autorizzata allo scopo di incrementare l'efficienza e «ridurre i tempi di definizione dei procedimenti», dall'altro il legislatore statuisce in modo inequivocabile che il suo impiego deve avvenire esclusivamente «in funzione strumentale e di supporto all'attività» umana. L'articolo 14 erige a dovere istituzionale la trasparenza algoritmica, imponendo alle amministrazioni di assicurare sempre agli interessati «la conoscibilità del suo funzionamento e la tracciabilità del suo utilizzo», ribadendo che il potere e la responsabilità della decisione finale non possono mai essere delegati alla macchina.

La chiusura del cerchio regolatorio avviene sul piano strettamente operativo attraverso le Linee Guida AgID per l'adozione, l'acquisto e lo sviluppo di sistemi di IA nella Pubblica Amministrazione, previste dall'articolo 71 del Codice dell'Amministrazione Digitale e dal Piano Triennale per l'informatica nella PA. Proprio il Codice dell'Amministrazione Digitale, peraltro, è attualmente al centro di un processo di profondo aggiornamento strutturale, finalizzato ad adeguarne l'impianto alle inedite sfide imposte dall'innovazione tecnologica. A testimonianza di questa vitale transizione istituzionale, nel febbraio del 2026 è stata istituita un'apposita Commissione per la revisione del Codice dell'amministrazione digitale e per la disciplina per le modalità digitali dell'attività di produzione normativa, la cui presidenza è stata affidata al Prof. Aristide Police. Questo cantiere riformatore conferma in modo inequivocabile l'esigenza di un ecosistema normativo dinamico, capace di dialogare costantemente con il progresso tecnico.

È all'interno di questa cornice in rapida evoluzione che si inserisce il ruolo delle citate Linee Guida AgID. Esse traducono la norma giuridica in standard tecnici e protocolli organizzativi: pur appartenendo formalmente alla categoria della soft law, nella prassi amministrativa assumono una funzione sostanzialmente vincolante, poiché definiscono i requisiti di conformità necessari per l'acquisizione e l'esercizio dei sistemi algoritmici. È attraverso questi standard che i principi di trasparenza e responsabilità si trasformano in requisiti informatici concreti di auditabilità, tracciabilità e registrazione dei log di funzionamento, consentendo la ricostruzione ex post del processo decisionale.

Questa infrastruttura normativa integrata ha un fine preciso: costruire fiducia istituzionale. Essa mira a evitare che l'innovazione generi “zone grigie” nelle quali il potere pubblico operi al di fuori delle garanzie del procedimento amministrativo. L'uso sommerso dell'IA non rappresenta soltanto un rischio tecnologico, ma un indicatore di immaturità della governance: segnala il ritardo con cui il diritto e le organizzazioni amministrative riescono a incorporare innovazioni che, nella prassi quotidiana degli uffici, sono già divenute operative.

3. Il ruolo della difesa civica

Nuovi orizzonti nella tutela dei diritti

Nel contesto della nuova architettura regolatoria dell'intelligenza artificiale delineata a livello europeo e nazionale, anche le istituzioni di garanzia sono chiamate a ridefinire il proprio ruolo.

Nell'attuale panorama istituzionale, la missione del Difensore civico sta conoscendo una trasformazione profonda. È bene ricordare che il Difensore è, prima di tutto, un organo di garanzia autonomo e indipendente, il cui raggio d'azione si dispiega non solo nei confronti della Pubblica Amministrazione, ma — in molti ordinamenti, tra cui quello italiano — si estende anche ai soggetti privati che gestiscono servizi pubblici essenziali. Questa peculiare collocazione “a metà strada” tra il cittadino e l'apparato amministrativo, caratterizzata da funzioni di moral suasion e di composizione non giurisdizionale dei conflitti, non costituisce un residuo nostalgico di un'epoca pre-digitale. Al contrario, proprio la flessibilità di questo ruolo lo rende uno degli strumenti istituzionali più adatti a operare lungo la nuova frontiera immateriale della tutela.

La burocrazia tradizionale non scompare: continua a esistere nei suoi riti, nei suoi tempi e nelle sue forme organizzative. Tuttavia, accanto alla dimensione materiale degli uffici e degli atti amministrativi si sviluppa una seconda dimensione, meno visibile ma sempre più decisiva, nella quale l'apparato pubblico prende forma attraverso sistemi informatici, piattaforme digitali e procedure automatizzate. Se il cittadino continua a incontrare l'amministrazione negli sportelli, nei moduli e nei provvedimenti formali, sempre più spesso la decisione che lo riguarda si forma all'interno di processi informativi che operano “a monte” dell'atto finale, organizzando le priorità, i tempi e le modalità di trattazione delle istanze.

La letteratura ha spesso rappresentato la materialità della burocrazia attraverso l'immagine della sequenza interminabile di timbri e certificazioni. Ennio Flaiano la descriveva come una sorta di liturgia amministrativa, fatta di atti che si moltiplicano e si legittimano reciprocamente, evocando quella “calata dei timbri” che, più che garantire la decisione, sembra talvolta sostituirla.

Nelle procedure amministrative caratterizzate da elevata serialità — come i servizi anagrafici, l'erogazione di prestazioni assistenziali, l'assegnazione di alloggi di edilizia residenziale pubblica o la gestione di agevolazioni tariffarie — sistemi algoritmici adeguatamente progettati possono effettivamente incrementare la capacità di trattazione delle istanze, ridurre i tempi di risposta e contenere gli arretrati. In tali contesti, l'automazione può contribuire a migliorare l'efficienza organizzativa e a garantire maggiore uniformità nell'applicazione dei criteri normativi.

Tuttavia, l'efficienza non esaurisce il parametro di legittimità e di qualità dell'azione amministrativa. La realtà presenta inevitabilmente situazioni non pienamente riconducibili a schemi predeterminati: disallineamenti tra banche dati, condizioni soggettive atipiche, errori materiali o circostanze che richiedono una valutazione interpretativa della norma. In questi casi, un sistema rigidamente parametrico può produrre esiti formalmente coerenti ma sostanzialmente inadeguati rispetto alla complessità del caso concreto.

Per questa ragione, l'introduzione dell'IA nei procedimenti amministrativi richiede presidi chiari: trasparenza dei criteri utilizzati, possibilità di intervento umano effettivo, strumenti di rettifica e canali accessibili di riesame. La tecnologia può supportare la decisione, ma non può esaurirne la responsabilità.

In tale contesto, il ruolo del Difensore civico, esattamente come accade per la politica, non deve iscriversi né al partito degli entusiasti né a quello dei catastrofisti. Deve assumere semplicemente la funzione di garanzia che gli è propria, verificando che l'impiego di strumenti algoritmici non comporti compressioni indebite dei diritti, assicurare che nei casi non standardizzati sia effettivamente possibile un riesame umano e contribuire a mantenere un equilibrio tra efficienza organizzativa e tutela sostanziale della persona.

Se l'automazione consente agli uffici di alleggerire la gestione delle pratiche seriali, ciò può tradursi in una maggiore disponibilità di risorse per i casi complessi e per le situazioni che richiedono ascolto e valutazione personalizzata. In questa prospettiva, tecnologia e tutela non si pongono in alternativa, ma devono essere integrate entro un assetto in cui la velocità operativa non prevalga sulla giustizia del caso concreto, né la cautela paralizzi l'innovazione organizzativa.

Questa trasformazione modifica l'oggetto stesso della tutela. Tradizionalmente, il controllo si è concentrato sull'atto amministrativo finale, quale manifestazione giuridica della volontà dell'ente. Oggi, tuttavia, una parte crescente del procedimento prende corpo molto prima, all'interno di passaggi istruttori automatizzati o governati da software. Pensiamo a casi concreti: la gestione automatizzata delle liste di attesa sanitarie, l'assegnazione delle priorità per l'accesso a prestazioni sociali, lo smistamento delle istanze di accesso agli atti, la selezione delle pratiche da evadere o l'organizzazione delle code digitali nei servizi pubblici. In questi contesti, è nella filiera informatica del procedimento che si determinano i tempi, si accumulano i ritardi e si producono i silenzi amministrativi. L'atto finale rischia così di ridursi a una mera "veste giuridica" che ratifica una valutazione già compiuta in precedenza.

Se il Difensore civico si limitasse a intervenire a valle, arriverebbe quando il danno è già cristallizzato. La vera sfida consiste invece nell'estendere lo sguardo all'interno delle procedure informatizzate, rivendicando l'accessibilità, la comprensibilità e la verificabilità delle logiche che governano il software pubblico.

La letteratura e l'immaginario collettivo hanno più volte rappresentato l'impotenza del cittadino di fronte ai meccanismi amministrativi: dal labirinto del Castello di Kafka alla celebre "Casa che rende

folli” nella quale Asterix e Obelix sono costretti a inseguire un lasciapassare A38. La digitalizzazione non elimina il rischio di questi labirinti: può anzi renderli più silenziosi e meno visibili, trasformando la complessità procedurale in opacità algoritmica.

Di fronte al rischio di *black box decision-making*, il Difensore civico è chiamato ad assumere il ruolo anche di garante della trasparenza tecnica. Quando l'amministrazione giustifica una esclusione o un ritardo richiamando semplicemente l'esito del sistema informatico, il Difensore deve pretendere la tracciabilità della “contaminazione tecnologica”, verificando che l'algoritmo non celi *bias* discriminatori derivanti da dati storici distorti e che sia possibile ricostruire a ritroso il percorso logico della decisione.

Questa esigenza di ricostruzione a ritroso non risponde a un mero vezzo tecnologico, ma incide direttamente sul nucleo fondante dello Stato di diritto: l'obbligo di motivazione sancito dall'articolo 3 della Legge 7 agosto 1990, n. 241. La dottrina e la più autorevole giurisprudenza amministrativa convergono nel ritenere che un provvedimento fondato su un algoritmo inaccessibile sia radicalmente illegittimo, in quanto privo del contenuto minimo essenziale della motivazione. Il Consiglio di Stato, con le pronunce capostipite della Sezione VI (in particolare le sentenze n. 2270 e n. 8472 del 2019), ha chiarito in modo inequivocabile che il software deve essere considerato a tutti gli effetti come un «atto amministrativo informatico» e che l'algoritmo va qualificato giuridicamente come un «modulo procedimentale».

Da questa precisa qualificazione discende che la regola algoritmica, pur declinata in forma matematica, deve soggiacere ai principi generali dell'attività amministrativa: la motivazione del provvedimento deve necessariamente tradursi nell'esplicazione della logica informatica adottata (*explainability*). Un atto che si limiti a recepire passivamente un output generato da un sistema opaco impedisce di ripercorrere l'iter logico-giuridico seguito dall'ente, vanificando la funzione di garanzia della motivazione e precludendo ogni effettivo diritto di difesa per il cittadino.

Tuttavia, l'inquadramento dell'algoritmo come atto amministrativo teoricamente ostensibile pone un interrogativo dirimente sul piano squisitamente operativo: il Difensore civico possiede le competenze necessarie per valutare e decidere su un riesame riguardante un'istanza di accesso agli atti che abbia ad oggetto, ad esempio, il codice sorgente di un software o i file di log di un sistema decisionale automatizzato?

Di fronte a un'amministrazione che nega l'accesso al cittadino opponendo la tutela del segreto industriale, del diritto d'autore o l'impenetrabilità di un'architettura informatica acquisita "chiavi in mano" da un fornitore privato, il bagaglio del puro giurista rischia di non essere più sufficiente. Affinché la risposta all'istanza di riesame non si riduca a un asseveramento formale dei limiti tecnici opposti dall'ente, la difesa civica del futuro dovrà necessariamente aprirsi a una rigorosa contaminazione interdisciplinare. Sarà indispensabile integrare competenze tecnico-informatiche capaci di supportare

l'Ufficio nel delicatissimo bilanciamento tra il diritto pubblico alla trasparenza (*explainability*) e i vincoli commerciali o di sicurezza legati al codice informatico.

In questo modo la difesa civica contribuisce a contrastare il rischio di un vuoto di responsabilità, ribadendo che dietro ogni errore — anche quando mediato da sistemi automatizzati e tutelati da barriere tecniche — permane sempre una responsabilità istituzionale umana e organizzativa pienamente sindacabile.

Ma l'intelligenza artificiale non è soltanto un oggetto da controllare: può diventare anche uno strumento di tutela attiva. Gli uffici dei Difensori civici ricevono quotidianamente un flusso imponente ed eterogeneo di segnalazioni — e-mail, PEC, telefonate, istanze digitali — spesso redatte in condizioni di forte stress emotivo, nelle quali fatti oggettivi e percezioni soggettive si intrecciano rendendo complessa l'individuazione immediata delle questioni giuridicamente rilevanti. In questa fase di “triage”, l'IA può fungere da infrastruttura di ordinamento logico. Strumenti avanzati di elaborazione del linguaggio naturale possono estrarre automaticamente gli elementi essenziali delle doglianze, individuando ricorrenze lessicali che segnalano categorie di disagio tipiche — ritardi cronici, dinieghi di accesso, errori materiali o disfunzioni sistemiche — e consentendo così di cogliere pattern ricorrenti difficilmente individuabili attraverso l'analisi manuale dei fascicoli.

In questa prospettiva, l'intelligenza artificiale supporta il passaggio da una tutela episodica del singolo caso a una protezione sistemica dei diritti, permettendo al Difensore civico di individuare tempestivamente anomalie organizzative o disparità di trattamento territoriali e di intervenire prima che esse si traducano in contenziosi diffusi. Il cittadino non viene ridotto a un aggregato statistico, ma diventa il punto di partenza di un'azione istituzionale più informata, capace di trasformare l'ascolto individuale in conoscenza sistemica.

In conclusione, l'intelligenza artificiale non sostituisce il giudizio umano, ma lo potenzia. Liberando il Difensore civico dalle attività ripetitive di classificazione e analisi preliminare, consente di concentrare le risorse su ciò che nessun algoritmo potrà replicare: la capacità di ascolto, la gestione dell'eccezione complessa, la mediazione tra amministrazione e cittadino e la moral suasion istituzionale. Il Difensore civico del futuro non sarà un tecnico informatico, ma un giurista “aumentato”, capace di interrogare la tecnologia per costringerla a rispondere ai principi di legalità, giustizia e buon andamento dell'amministrazione.

4. Difesa civica e transizione digitale

Proposte e prassi operative

Al di là delle premesse teoriche, occorre verificare come i principi di trasparenza e responsabilità possano tradursi in prassi operative concrete all'interno di un ufficio di difesa civica moderno. Su questo punto, il confronto con autorevoli colleghi — dal Presidente del Coordinamento nazionale dei Difensori civici, Marino Fardelli, al Difensore civico della Regione Liguria, Francesco Cozzi — ha evidenziato una sostanziale concordia su un aspetto di fondo: non vi è alcuna necessità, né volontà, di “automatizzare” il giudizio. L'obiettivo dell'impiego dell'intelligenza artificiale è diverso e, solo apparentemente, meno ambizioso: evitare che l'attività di garanzia si disperda in una miriade di micro-attività a basso valore aggiunto — protocollazione, smistamento, catalogazione — che consumano tempo prezioso.

Lo scopo è liberare risorse cognitive per ciò che nessuna macchina può replicare: l'istruttoria sostanziale, l'ascolto empatico del cittadino e la complessa mediazione relazionale con l'amministrazione.

La fase di ingresso: dal triage al protocollo intelligente

Questi principi trovano una prima applicazione nella gestione dei flussi in entrata. L'esperienza di grandi amministrazioni come l'INPS — che gestisce milioni di PEC annue grazie a sistemi di classificazione automatica — dimostra come l'IA possa trasformare un problema di volume in un'opportunità di efficienza. Applicata all'Ufficio del Difensore civico, questa tecnologia permette di trasformare un racconto soggettivo e spesso disordinato (la mail del cittadino) in un dato strutturato. Un sistema di triage intelligente può leggere l'istanza, individuare l'amministrazione competente, proporre l'assegnazione al funzionario specializzato e, soprattutto, segnalare profili di urgenza. Non si decide “al posto” dell'ufficio, ma si prepara il terreno affinché l'intervento umano sia tempestivo.

Il filtro di ammissibilità

Una seconda applicazione cruciale riguarda la fase di pre-istruttoria. Il Difensore civico è tenuto a verificare preliminarmente la propria competenza e l'assenza di cause ostative (es. questioni penali, liti tra privati). In questa fase, l'IA può agire come un filtro di supporto, eseguendo controlli formali che sollevano l'ufficio dai compiti più meccanici:

- Verifica della legittimazione: Analisi preliminare dell'interesse ad agire.

- Perimetro di competenza: Mappatura automatica degli enti vigilati, scartando istanze rivolte ad amministrazioni statali o organi giudiziari.
- Calcolo dei termini: Verifica computistica della tempestività (es. il rispetto dei 30 giorni per il riesame dell'accesso agli atti), rilevando immediatamente eventuali tardività. Il sistema non rigetta l'istanza, ma segnala l'incoerenza al funzionario, predisponendo una scheda di ammissibilità che l'operatore umano dovrà solo validare.

L'istruttoria: ricostruzione normativa e tutela sistemica

Nel cuore del procedimento, l'istruttoria, l'IA evolve da filtro ad assistente di ricerca. La difesa civica vive di ricostruzione dei fatti e delle norme. Qui, algoritmi di ricerca semantica possono supportare la ricostruzione del quadro normativo, evidenziando disposizioni abrogate o modifiche recenti, e ordinare cronologicamente la documentazione (creando un vero e proprio "dossier vivo"), facendo emergere discrepanze tra quanto dichiarato e quanto provato.

Ma il vero salto di qualità è la tutela sistemica. Quando il software evidenzia che decine di fascicoli presentano la medesima anomalia (ad esempio, un ritardo standardizzato in uno specifico ufficio o il rigetto seriale di un'istanza), il Difensore non si trova più di fronte a un disservizio episodico, ma all'emersione di una *maladministration* strutturale.

Che l'intelligenza artificiale possa fungere da strumento per valutare la qualità dell'azione pubblica non è, peraltro, una mera suggestione teorica. Una dimostrazione concreta e pionieristica in questa direzione è offerta dal progetto SAVIA (Intelligenza artificiale per la qualità delle leggi), ideato dall'Assemblea legislativa della Regione Emilia-Romagna in collaborazione con il CINECA. Attraverso l'uso di modelli linguistici avanzati (LLM), SAVIA interroga le banche dati regionali per supportare il legislatore nella valutazione ex ante ed ex post dell'impatto delle norme, garantendo al contempo maggiore trasparenza e partecipazione per la comunità.

Mutuando esattamente questo stesso approccio analitico e traslandolo dal campo della produzione legislativa a quello della tutela dei diritti, l'intelligenza artificiale permette al Difensore civico di compiere un passo decisivo: passare definitivamente dalla cura del singolo sintomo alla diagnosi della patologia amministrativa.

Questa capacità diagnostica apre la strada a una delle applicazioni più promettenti dell'intelligenza artificiale generativa al servizio delle istituzioni: la pianificazione degli scenari. L'IA, infatti, può elaborare rapidamente enormi quantità di dati storici e precedenti amministrativi per creare "bozze di scenari" predittivi. Questa evoluzione si rivela fondamentale per l'esercizio della funzione di garanzia: che si tratti di prevedere l'impatto di un improvviso cambio nei criteri di accesso all'edilizia residenziale pubblica, o di anticipare l'ondata di segnalazioni derivante dall'introduzione di un nuovo e complesso

sistema di tariffazione locale, la GenAI può simulare rapidamente le ricadute sui cittadini basandosi su eventi analoghi del passato.

In questo modo, il ruolo del Difensore civico fa un ulteriore passo in avanti: la modellazione predittiva consente di superare la logica dell'intervento *ex post*, permettendo all'Ufficio di allertare l'amministrazione in via preventiva e di suggerire misure organizzative prima che la criticità procedurale si trasformi in una lesione conclamata e diffusa dei diritti dei cittadini.

La fase decisionale

Giungiamo infine al momento decisivo e più delicato dell'intero iter procedurale: la redazione dell'atto finale, sia esso un invito a ottemperare, una raccomandazione o un'archiviazione. In questo snodo, la cautela deve essere massima. Come chiarito anche dal Regolamento UE 2024/1689 (il cosiddetto AI Act), i sistemi di intelligenza artificiale destinati a supportare le decisioni amministrative o le funzioni di garanzia ricadono tendenzialmente nella classificazione ad "Alto Rischio". Tuttavia, lo stesso legislatore europeo distingue con pragmatica saggezza tra le "attività accessorie" — ammesse con un minor rigore formale — e la "decisione effettiva". L'intelligenza artificiale può certamente supportare la stesura formale, migliorare la chiarezza espositiva del linguaggio o verificare la coerenza logica con i precedenti dell'Ufficio, ma non potrà mai sostituire il giudizio di equità. L'atto del Difensore civico è, per sua intima natura, l'espressione di un delicato equilibrio istituzionale e di una sensibilità imparziale chiamata a valutare le innumerevoli sfumature del caso concreto, spesso irriducibili a una rigida logica binaria.

Anche la più autorevole giurisprudenza amministrativa ha tracciato con chiarezza questa via. Il Consiglio di Stato, con la nota sentenza della Sezione VI, n. 2270 dell'8 aprile 2019, ha affermato che l'automazione non deve essere demonizzata, ma anzi va incoraggiata qualora consenta di ridurre la negligenza o il dolo umano, a una condizione essenziale: che non si abdichi mai ai principi cardine di trasparenza e motivazione. L'algoritmo, in definitiva, non è un oracolo misterioso e insindacabile, ma una mera "regola tecnica" che deve rimanere sempre intelligibile e contestabile.

Negli anni successivi, i principi fissati dall'Adunanza Plenaria in materia di algoritmi sono stati spesso oggetto di opposte strumentalizzazioni, contesi tra i "tifosi" della totale automazione e i detrattori aprioristici del mezzo tecnologico. Tuttavia, con la capillare diffusione dei sistemi basati su modelli linguistici di grandi dimensioni (LLM), abbiamo assistito a una progressiva maturazione del dibattito e a pronunce giurisprudenziali più equilibrate, capaci di collocarsi "nel mezzo" tra questi due estremi.

In questo quadro evolutivo si inserisce il recente orientamento del TAR Lazio (espresso, da ultimo, nella sentenza n. 1895/2026), il quale ha chiarito come l'automatismo procedimentale non possa mai tradursi in una cieca espulsione del dato utile o nell'esclusione di un vaglio critico sull'output della macchina.

Nelle decisioni amministrative digitalizzate resta imprescindibile quella che viene definita "riserva di umanità", ovvero una human oversight (supervisione umana) effettiva e penetrante.

L'Amministrazione, in ogni sua articolazione, deve mantenere un controllo reale e la piena capacità di intervenire sulle decisioni generate dai sistemi automatizzati. Questo imperativo si fonda sui pilastri costituzionali del nostro ordinamento (gli artt. 3, 24 e 97 della Costituzione), nonché sulle solide garanzie della Legge 241/1990 e del Codice dell'Amministrazione Digitale. In tale contesto, l'AI Act assume un ruolo cruciale: pur non trovando sempre un'applicazione diretta al singolo micro-procedimento interno, esso funge da potente "parametro interpretativo evolutivo". La sua ratio rafforza l'obbligo di trasparenza e la piena sindacabilità delle decisioni algoritmiche, specialmente laddove si impieghino sistemi ad alto rischio, come avviene nelle selezioni pubbliche. Ne consegue che persino il rigido principio di autoresponsabilità del cittadino subisce un'attenuazione laddove il requisito sostanziale sia comunque riscontrabile e l'errore derivi unicamente da una rigidità del software.

In conclusione, l'intelligenza artificiale entra nell'Ufficio del Difensore civico non assumendo le vesti di un giudice algoritmico inflessibile, ma ponendosi come uno strumento di governo della complessità. La tecnologia solleva l'istituzione dal peso burocratico e formale, permettendo all'Ombudsman di rimanere fedele alla sua missione originaria: garantire, con ponderazione e indipendenza, che anche in un mondo profondamente digitalizzato la Pubblica Amministrazione conservi sempre un volto umano.

5. Conclusioni

L'analisi sviluppata nelle pagine precedenti consente di partire da una constatazione semplice, ma spesso trascurata nel dibattito pubblico: l'intelligenza artificiale è già entrata nella quotidianità delle amministrazioni pubbliche. Non attraverso grandi sistemi decisionali formalmente introdotti, ma tramite una molteplicità di utilizzi individuali, diffusi e spesso invisibili all'amministrazione.

Questa dinamica rende poco realistico affrontare il fenomeno esclusivamente in termini proibitivi. Quando l'amministrazione si limita a vietare l'uso dell'intelligenza artificiale senza offrire strumenti istituzionali alternativi, l'effetto non è l'eliminazione della tecnologia, ma la sua migrazione verso forme informali di utilizzo. I dipendenti continuano a ricorrervi tramite dispositivi personali o account privati, talvolta inserendo informazioni sensibili all'interno di piattaforme esterne sulle quali l'ente non esercita alcun controllo. Paradossalmente, il tentativo di difendere l'organizzazione dal rischio tecnologico finisce così per indebolire proprio quelle garanzie di sicurezza e tracciabilità che si intendeva preservare.

Il problema, dunque, non è se l'intelligenza artificiale debba essere utilizzata, ma come essa possa essere ricondotta entro una cornice istituzionale governata. La vera alternativa non è tra uso e divieto, ma tra un uso spontaneo, individuale e opaco e un uso istituzionale, disciplinato e responsabile.

In questo quadro, la questione delle competenze assume un rilievo che va oltre la dimensione puramente tecnica. La progressiva digitalizzazione dei procedimenti amministrativi implica che una parte crescente delle decisioni pubbliche si formi all'interno di infrastrutture informative e sistemi di elaborazione dei dati. Comprendere il funzionamento di tali sistemi non significa trasformare i giuristi in ingegneri informatici, ma evitare che le decisioni giuridiche vengano progressivamente condizionate da strumenti tecnologici che restano opachi a chi li utilizza.

Per le istituzioni di garanzia, e in particolare per la difesa civica, questa trasformazione assume un significato ancora più profondo. L'Ombudsman è nato storicamente per contrastare le rigidità e le opacità della burocrazia tradizionale, offrendo al cittadino uno spazio di interlocuzione capace di ricondurre l'azione amministrativa entro parametri di equità e ragionevolezza.

Oggi, tuttavia, una parte crescente delle decisioni amministrative non si forma più esclusivamente nell'atto finale, ma prende corpo all'interno di procedure digitali, sistemi informativi e logiche algoritmiche che operano a monte del provvedimento formale. In questo contesto, il rischio non è soltanto l'errore amministrativo, ma la progressiva incomprensibilità dei processi decisionali.

La funzione di garanzia della difesa civica è quindi destinata a misurarsi sempre più con questa dimensione invisibile dell'azione amministrativa. Non per sostituirsi alle amministrazioni nella gestione tecnologica dei sistemi, ma per assicurare che anche nell'ambiente digitale restino effettivi i principi

fondamentali dello Stato di diritto: comprensibilità delle decisioni, responsabilità delle istituzioni e possibilità di contestazione da parte dei cittadini.

In questa prospettiva, oltre a strumento di regolazione o di controllo, l'intelligenza artificiale può diventare anche un supporto all'attività di garanzia, consentendo di analizzare grandi flussi di segnalazioni, individuare anomalie ricorrenti e trasformare l'esperienza del singolo caso in conoscenza sistemica sulle disfunzioni amministrative.

Il nodo centrale resta tuttavia di natura istituzionale. L'intelligenza artificiale non sostituisce la responsabilità pubblica; al contrario, la rende ancora più necessaria. Quanto più i processi amministrativi si affidano a sistemi complessi di elaborazione dei dati, tanto più diventa essenziale preservare spazi di comprensione, controllo e responsabilità.

La sfida che si apre per le amministrazioni e per le istituzioni di garanzia non consiste quindi nel decidere se utilizzare o meno l'intelligenza artificiale, ma nel definire le condizioni entro cui essa possa essere integrata senza alterare l'equilibrio tra efficienza amministrativa e tutela dei diritti.

In questo senso, il tema dell'intelligenza artificiale nella P.A. non riguarda soltanto l'innovazione tecnologica, ma la capacità delle istituzioni di adattarsi a un ambiente decisionale sempre più complesso senza smarrire i principi che fondano la legittimità dell'azione amministrativa.