DIFENSORE CIVICO della REGIONE LAZIO

CONSIGLIO REGIONALE DEL LAZIO

Il Difensore Civico nell'era dell'Intelligenza Artificiale

Diritti e tecnologie emergenti: un approccio strategico, predittivo e trasformativo alla tutela dei diritti

Marino Fardelli

Guido Giusti

Ignacio Domínguez

Il Difensore Civico nell'era dell'Intelligenza Artificiale

Diritti e tecnologie emergenti: un approccio strategico, predittivo e trasformativo alla tutela dei diritti

Marino Fardelli

Difensore civico della Regione Lazio
Presidente del Coordinamento Nazionale dei Difensori Civici italiani

Guido Giusti

Difensore civico della Regione Emilia-Romagna
Vicepresidente del Coordinamento Nazionale dei Difensori Civici italiani

Ignacio Domínguez

Direttore e CEO di Yakatiak, Consulenti e Associati - Messico
Intelligenza Artificiale, Calcolo Quantistico e Sicurezza Informatica

Indice

Introduzione

Riflessioni di un Difensore Civico

(Marino Fardelli)

Scrivere oggi di Intelligenza Artificiale, diritti e tecnologie emergenti dal punto di vista di un Difensore Civico significa assumersi una responsabilità che travalica i confini dell'analisi istituzionale in senso stretto. Significa, più profondamente, interrogarsi sul senso e sulla funzione del ruolo di garanzia in una fase storica caratterizzata da un evidente disallineamento tra la velocità del progresso tecnologico e la capacità dell'ordinamento — così come delle istituzioni e delle stesse comunità — di comprenderlo, governarlo e orientarlo. È una responsabilità che si colloca all'intersezione tra diritto, etica pubblica e governo dell'innovazione.

Il Difensore Civico nasce come presidio di prossimità: ascolta, media, tutela, riequilibra. La sua legittimazione si è progressivamente costruita sul rapporto diretto con il cittadino, sulla capacità di restituire misura e umanità là dove la burocrazia rischia di trasformarsi in distanza e il procedimento amministrativo in un meccanismo autoreferenziale, potenzialmente disancorato dalla persona. Tuttavia, nell'attuale contesto tecnologico, tale funzione non può più esaurirsi in una logica meramente reattiva, limitata all'intervento ex post rispetto a una lesione già verificatasi.

L'avvento dell'Intelligenza Artificiale, lo sviluppo dell'informatica quantistica e la crescente centralità della sicurezza informatica impongono un mutamento di paradigma: da un modello di tutela fondato sulla risposta al conflitto a un modello orientato alla prevenzione, all'anticipazione e alla gestione dei rischi sistemici. In questa prospettiva, il Difensore Civico è chiamato a evolvere verso una funzione anche strategica e predittiva, capace di intercettare precocemente le criticità generate dall'uso delle tecnologie e di contribuire alla costruzione di un ecosistema amministrativo più equo, trasparente e resiliente.

Non si tratta soltanto di risolvere controversie individuali, ma di presidiare fenomeni complessi: prevenire nuove forme di disuguaglianza digitale, contrastare dinamiche discriminatorie generate da sistemi algoritmici opachi, vigilare su possibili compressioni silenziose dei diritti fondamentali. L'asimmetria informativa tra amministrazione e cittadino, già rilevante nei contesti tradizionali, rischia infatti di amplificarsi ulteriormente in presenza di sistemi decisionali automatizzati, nei quali l'opacità tecnica può tradursi in opacità giuridica.

Le tecnologie emergenti stanno ridisegnando in profondità il rapporto tra cittadino e pubblica amministrazione, tra individuo e potere decisionale, tra libertà e controllo. Algoritmi che attribuiscono punteggi o priorità, sistemi automatizzati che orientano decisioni pubbliche, infrastrutture digitali che concentrano e trattano enormi quantità di dati personali e non personali: tutto ciò estende in modo significativo la capacità d'azione dell'amministrazione, ma ne accresce, al contempo, le aree di vulnerabilità. Il rischio non è solo quello dell'errore, ma anche quello della non contestabilità effettiva delle decisioni, quando queste risultino fondate su logiche non pienamente conoscibili o verificabili.

In tale scenario, il Difensore Civico non può limitarsi a un ruolo di osservatore. È chiamato a porsi quale interprete qualificato del cambiamento, garante della trasparenza e della spiegabilità algoritmica, custode dell'equità digitale e presidio avanzato dei diritti nell'ecosistema tecnologico. Ciò implica anche un rafforzamento delle competenze: accanto al sapere giuridico tradizionale, diventa imprescindibile una adeguata alfabetizzazione tecnologica, idonea a comprendere - almeno nelle loro linee essenziali - le logiche di funzionamento dei sistemi digitali.

Accanto a questa dimensione istituzionale, si innesta inevitabilmente una riflessione personale. Mai avrei immaginato che, dopo aver discusso una tesi di laurea dal titolo "Servizi telematici nell'educazione e formazione", mi sarei ritrovato, a distanza di oltre ventisei anni, ad affrontare in chiave istituzionale il tema del rapporto tra diritti e tecnologia. All'epoca, i servizi telematici rappresentavano una promessa: connessioni lente, strumenti ancora embrionali, una visione del futuro che si collocava più nell'ambito della possibilità che in quello della realtà.

Oggi, quel futuro si è pienamente realizzato, e in forme spesso impreviste. Il progresso tecnologico non è più soltanto un vettore di opportunità, ma si configura come un ambito intrinsecamente ambivalente, che richiede responsabilità, capacità di governo e consapevolezza diffusa. Se da un lato esso consente di migliorare l'efficienza, l'accessibilità e la qualità dei servizi pubblici, dall'altro lato pone questioni inedite in termini di tutela dei diritti, di controllo democratico e di accountability delle decisioni automatizzate.

Guardando al passato e al presente, colpisce certamente la rapidità del cambiamento. Ma, ancor più, colpisce la permanenza di alcuni elementi fondamentali: il bisogno di tutela della persona, la centralità della dignità umana, l'esigenza di istituzioni capaci di farsi carico delle fragilità e di garantire l'effettività dei diritti. Mutano i contesti, gli strumenti e i linguaggi; i diritti, invece, restano il punto di riferimento imprescindibile attorno a cui deve continuare a ruotare l'azione pubblica.

Questo lavoro nasce proprio da tale consapevolezza: l'innovazione tecnologica non è neutrale e, in assenza di una governance orientata ai diritti, rischia di amplificare squilibri già esistenti o di generarne di nuovi. In questa prospettiva, il Difensore Civico, nell'orizzonte 2026–2030, è chiamato a collocarsi in uno spazio inedito, in cui competenze giuridiche, sensibilità sociale e conoscenze tecnologiche devono integrarsi in modo strutturale e continuo.

Intelligenza Artificiale, informatica quantistica e sicurezza informatica non rappresentano ambiti estranei rispetto alla difesa civica: costituiscono, piuttosto, i nuovi terreni sui quali si giocherà la concreta ed effettiva tutela dei diritti dei cittadini. È in tali spazi che si definirà la capacità delle istituzioni di rimanere fedeli ai principi di legalità, imparzialità e buon andamento, anche in presenza di processi decisionali sempre più complessi e mediati dalla tecnologia.

Le presenti pagine non intendono offrire soluzioni definitive, né proporsi come trattazione esaustiva di temi in continua evoluzione. Esse si pongono, più modestamente ma non meno ambiziosamente, l'obiettivo di aprire una riflessione, stimolare un confronto e delineare una possibile traiettoria: quella di un Difensore Civico capace non di inseguire l'innovazione, ma di accompagnarla, orientarla e, ove necessario, sottoporla a un vaglio critico rigoroso.

Il futuro dei diritti non si costruisce opponendosi alla tecnologia, ma governandola con intelligenza, responsabilità e visione. Ciò significa accompagnare i processi innovativi senza subirli, prevenire l'insorgere di nuove forme di disuguaglianza e promuovere un modello di sviluppo tecnologico che sia inclusivo, equo e consapevole, in linea con i principi fondamentali dell'ordinamento.

A supporto di questa riflessione, il presente lavoro si arricchisce dei contributi di alto valore giuridico e tecnico dei miei compagni di viaggio, l'Avv. Guido Giusti e il Dott. Ignacio Domínguez. Ci siamo conosciuti durante una sessione di lavoro dedicata alle buone pratiche, in occasione di una conferenza internazionale degli Ombudsman, e ho avuto modo di constatare direttamente come il valore delle relazioni professionali possa tradursi in un'effettiva capacità di mettere in rete esperienze, competenze e prospettive differenti.

In un contesto caratterizzato da sfide globali e interconnesse, la collaborazione tra giuristi, tecnici e istituzioni non rappresenta un elemento accessorio, ma una condizione essenziale per governare i processi in atto. È proprio attraverso tali sinergie che diventa possibile trasformare la complessità in opportunità e rendere la cooperazione uno strumento concreto di tutela dei diritti nell'era delle tecnologie emergenti.

PARTE PRIMA

Difesa civica, trasparenza e governo dell'algoritmo.

L'ESPERIENZA ITALIANA.

Capitolo 1

L'INTELLIGENZA ARTIFICIALE NELLA PUBBLICA AMMINISTRAZIONE.

(Guido Giusti)

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, in Italia 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.

Capitolo 2

SUPERARE LA CRISI DELLA GOVERNANCE

(Guido Giusti)

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.

Capitolo 3

IL RUOLO DELLA DIFESA CIVICA

(Guido Giusti)

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 presìdi 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 inconoscibile 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 assecondamento 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 tute-

la 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.

Capitolo 4

DIFESA CIVICA E TRANSIZIONE DIGITALE

(Guido Giusti)

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 par-

tecipazione 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.

L'intelligenza artificiale entra nell'Ufficio del Difensore civico non assumendo le vesti di un giudice algoritmico, ma ponendosi come uno strumento di governo della complessità. La tecnologia può, infatti, sollevare 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.

Capitolo 5

CONSIDERAZIONI CONCLUSIVE

(Guido Giusti)

Come abbiamo visto nelle nelle pagine precedenti , l'intelligenza artificiale è già entrata nella quotidianità delle amministrazioni pubbliche 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 procedu-

re 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. amministrazione 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.

PARTE SECONDA

NUOVE TECNOLOGIE E NUOVE FRONTIERE DELLA TUTELA.

Capitolo 1

L'INTELLIGENZA ARTIFICIALE A FAVORE DELLA DIFESA CIVICA E DEI DIRITTI UMANI

(Ignacio Domínguez)

La difesa e la tutela dei diritti umani stanno attraversando oggi una trasformazione profonda. Il contesto globale — segnato da una digitalizzazione accelerata, da una crisi di fiducia nelle istituzioni, da conflitti complessi e da nuove forme di violazione dei diritti — esige che le istituzioni di Ombudsman evolvano con pari rapidità e responsabilità. In questo scenario, le nuove tecnologie cessano di essere una risorsa opzionale per diventare strumenti strategici al servizio della dignità umana, della democrazia e dello Stato di diritto.

Cominciamo con un'idea semplice:

i diritti umani non sono un archivio. Non sono una pratica amministrativa. Non sono un rapporto annuale. Sono persone reali, in tempo reale, che si confrontano con il potere.

Per decenni, gli Ombudsman del mondo sono stati la coscienza dello Stato. Hanno osservato, ascoltato, documentato. Hanno difeso. E questo è stato essenziale. Ma oggi non è più sufficiente. Il mondo è cambiato.

Viviamo in un'epoca in cui le decisioni si prendono in millisecondi, in cui i dati crescono in modo esponenziale e in cui la tecnologia può amplificare tanto la giustizia quanto l'ingiustizia. In questo nuovo scenario, la domanda non è se le istituzioni per i diritti umani debbano utilizzare la tecnologia. La vera domanda è: quale tipo di futuro vogliamo progettare?

L'intelligenza artificiale non è magia. È uno strumento. Ma, se utilizzata correttamente, è uno strumento straordinario.

Può aiutarci a individuare pattern dove prima vedevamo solo caos.

Può aiutarci ad anticipare violazioni prima che distruggano vite.

Può aiutarci a mettere la vittima al centro, non il fascicolo.

L'IA non sostituisce il giudizio umano: lo libera. Alleggerisce il peso delle attività ripetitive affinché possiamo concentrarci su ciò che conta davvero:

le persone.

Anche la cybersicurezza non è semplicemente una questione tecnica: è una questione di fiducia. Quando una persona affida la propria testimonianza a un Ombudsman, consegna qualcosa di più dei dati: consegna paura, speranza e verità. Se non proteggiamo queste informazioni, falliamo nel più basilare dei nostri doveri. Senza sicurezza digitale non c'è riservatezza, e senza riservatezza non ci sono diritti umani.

E poi c'è il calcolo quantistico.

Molti diranno: "non è ancora rilevante". È ciò che si dice sempre prima che il mondo cambi.

Il calcolo quantistico ridefinirà la sicurezza, la privacy e la protezione dell'informazione. Prepararsi oggi non è un'esagerazione: è responsabilità. I diritti umani non possono permettersi di arrivare tardi.

Oggi il calcolo quantistico è già una realtà: opera a livello commerciale in alcune aree dell'Asia già da prima del 2020 ed è da anni oggetto di utilizzo e sperimentazione da parte di organismi come la NASA e di grandi istituzioni finanziarie multinazionali. Anche in America Latina si registrano sviluppi concreti già a partire dal 2024.

Ma sia chiaro:

la tecnologia, da sola, non salva nessuno. Senza valori, senza etica, senza supervisione umana, può diventare fredda, opaca e pericolosa. Per questo, la vera sfida per gli Ombudsman del mondo non è tecnologica: è una sfida di leadership. Usare la tecnologia secondo principi. Progettare sistemi che rispettino la dignità umana. Decidere che gli algoritmi non siano mai al di sopra delle persone.

Le aree di opportunità sono evidenti e attendono di essere colte:

a) passare dalla reazione alla prevenzione;

b) dall'intuizione all'evidenza;

c) da istituzioni lente a istituzioni agili e umane;

d) da rapporti che guardano al passato a decisioni che costruiscono il futuro.

I benefici sono altrettanto evidenti: maggiore impatto, maggiore credibilità, maggiore fiducia, maggiore giustizia sostanziale.

Gli Ombudsman non sono chiamati a difendere processi, ma persone.

La tecnologia, se ben utilizzata, non disumanizza: fa esattamente il contrario. Restituisce tempo, chiarezza e concentrazione per essere più umani. Il futuro dei diritti umani non sarà scritto soltanto con le leggi: sarà progettato. E coloro che lo comprenderanno oggi - coloro che avranno il coraggio di unire etica, tecnologia e visione - non si limiteranno a proteggere i diritti, ma contribuiranno a trasformare il modo in cui il potere risponde alla dignità umana.

Questa è la sfida. Questa è l'opportunità. E, come sempre, il futuro appartiene a chi ha il coraggio di pensare in modo diverso.

Capitolo 2

LA DIFESA DEI DIRITTI E LA SFIDA DELLA CITTADINANZA DIGITALE

(Marino Fardelli)

Il nuovo ruolo dell'ombudsman

Le trasformazioni tecnologiche rappresentano una realtà quotidiana che incide in modo sempre più profondo sul rapporto tra cittadini e pubbliche amministrazioni. In questo scenario, la funzione dell'Ombudsman è chiamata a confrontarsi con sfide nuove, ma anche con opportunità inedite, che ne ridefiniscono progressivamente il perimetro e le modalità di intervento.

L'innovazione, infatti, non può essere considerata neutra. Essa incide sui procedimenti, modifica i linguaggi, accelera i tempi decisionali e, soprattutto, trasforma le modalità attraverso cui i diritti fondamentali vengono esercitati e tutelati. Per questa ragione, l'Ombudsman non può limitarsi a osservare il cambiamento: è chiamato a diventarne interprete consapevole e garante critico, affinché il progresso tecnologico rimanga costantemente orientato al servizio della persona.

In questo contesto, l'Intelligenza Artificiale sta progressivamente entrando nei processi decisionali della pubblica amministrazione, intervenendo nella gestione dei flussi informativi, nella selezione delle pratiche, nel supporto alle decisioni e nell'automazione delle risposte ai cittadini. Se da un lato tali strumenti possono contribuire a migliorare l'efficienza, la rapidità e l'uniformità dell'azione amministrativa, dall'altro pongono questioni rilevanti sotto il profilo della trasparenza, della spiegabilità delle decisioni e dell'imputazione delle responsabilità. Il rischio, non meramente teorico, è che l'algoritmo diventi uno schermo dietro cui l'amministrazione si sottrae al controllo, rendendo opaco ciò che dovrebbe restare accessibile e verificabile.

In tale prospettiva, il ruolo dell'Ombudsman assume una valenza strategica. È chiamato a vigilare affinché le decisioni automatizzate siano comprensibili e adeguatamente motivate, a garantire che l'utilizzo dell'intelligenza artificiale non produca effetti discriminatori - neppure in forma indiretta o involontaria - e ad assicurare che resti sempre possibile un intervento umano correttivo, soprattutto nei casi in cui siano coinvolti diritti fondamentali. L'intelligenza artificiale, in questa chiave, non deve sostituire il giudizio umano, ma affiancarlo e

sostenerlo, contribuendo a rafforzarne la qualità e l'equità.

Accanto all'IA, il calcolo quantistico rappresenta una delle più significative discontinuità tecnologiche del nostro tempo. Sebbene molte delle sue applicazioni siano ancora in fase di sviluppo, il suo potenziale impatto sui sistemi pubblici, sulla crittografia, sulla gestione dei dati e sulla sicurezza delle informazioni appare già oggi di portata rilevante. Per l'Ombudsman, il tema non si esaurisce nella dimensione tecnica, ma assume una chiara rilevanza istituzionale e prospettica. Ignorare il calcolo quantistico oggi significherebbe esporsi, nel prossimo futuro, a nuove vulnerabilità dei sistemi informativi pubblici, a rischi accresciuti per la protezione dei dati personali e a possibili squilibri di potere tra chi detiene tali tecnologie e chi ne subisce gli effetti.

Ne deriva l'esigenza di un approccio preventivo, orientato alla responsabilità pubblica dell'innovazione. L'Ombudsman è chiamato, in questa direzione, a promuovere una riflessione etica e giuridica che preceda l'affermazione definitiva delle tecnologie, evitando che scelte di grande impatto diventino irreversibili prima ancora di essere pienamente comprese e governate.

La cybersecurity, a sua volta, ha cessato da tempo di essere una questione confinata agli ambiti tecnici o militari, assumendo invece il ruolo di componente essenziale della tutela dei diritti. Un sistema pubblico vulnerabile espone i cittadini a rischi concreti e immediati: perdita di dati, violazioni della privacy, interruzioni di servizi essenziali, manipolazioni dell'informazione. In questo senso, la sicurezza informatica non può che essere considerata un presupposto imprescindibile per l'effettività dei diritti, strettamente connesso al principio di buon andamento dell'amministrazione.

All'interno di questo quadro, l'Ombudsman è chiamato a svolgere una funzione attiva, sollecitando l'adozione di standard elevati di protezione dei dati, segnalando criticità sistemiche che possano compromettere la fiducia dei cittadini e promuovendo una cultura della sicurezza digitale come elemento integrante della legalità amministrativa. La cybersicurezza, in questa prospettiva, non riguarda soltanto la difesa delle infrastrutture, ma la salvaguardia della relazione fiduciaria tra istituzioni e cittadini, che costituisce il fondamento stesso dell'azione pubblica.

In un contesto sempre più complesso e digitalizzato, la funzione dell'Ombudsman si arricchisce così di una dimensione ulteriore, assumendo i tratti di una mediazione evoluta. Non si tratta più soltanto di intervenire nel rapporto tra cittadino e amministrazione, ma anche di presidiare il delicato equilibrio tra innovazione tecnologica e diritti umani. Ciò richiede competenze multidisciplinari, capacità di dialogo con gli esperti tecnici senza smarrire la centralità della

persona e una visione etica dell'innovazione, orientata all'inclusione, alla trasparenza e alla responsabilità.

Le nuove tecnologie, se correttamente governate, non devono allontanare le istituzioni dai cittadini, ma possono costituire strumenti preziosi per avvicinarle. È proprio in questo spazio che l'Ombudsman può esercitare un ruolo decisivo, affermandosi come garante di un progresso capace di includere, e non di escludere.

Intelligenza Artificiale, calcolo quantistico e cybersecurity non sono più ambiti riservati agli specialisti, ma questioni che incidono direttamente sul funzionamento della democrazia contemporanea. In tale contesto, la funzione dell'Ombudsman, per sua natura indipendente e orientata alla tutela dei diritti, si configura come uno degli snodi istituzionali più idonei per accompagnare e orientare il cambiamento.

Governare l'innovazione, in definitiva, significa operare scelte consapevoli: privilegiare la trasparenza rispetto all'opacità, l'equità rispetto all'automatismo cieco, la sicurezza rispetto all'improvvisazione. In questo percorso, l'Ombudsman può — e deve — rappresentare una bussola affidabile, capace di orientare l'azione pubblica nel segno della dignità della persona.

Le raccomandazioni alla pubblica amministrazione

La tecnologia, se non accompagnata da una visione chiara e da una cultura amministrativa orientata al servizio, rischia di diventare un fattore di irrigidimento anziché di semplificazione. Digitalizzare procedure inefficaci significa spesso accelerare disfunzioni già esistenti, rendendole più difficili da correggere e meno comprensibili per i cittadini.

Quando l'Ombudsman interviene formulando raccomandazioni, l'attenzione non deve concentrarsi sullo strumento tecnologico in sé, ma sull'uso che l'amministrazione ne fa e sugli effetti concreti che esso produce sull'esercizio dei diritti. Le nuove tecnologie possono offrire un supporto rilevante all'azione amministrativa: migliorano la tracciabilità dei procedimenti, consentono una gestione più ordinata delle informazioni, riducono i tempi di risposta e favoriscono una maggiore trasparenza nelle decisioni. In questo senso, esse rappresentano un alleato prezioso anche per l'attività dell'Ombudsman, che può basare le proprie valutazioni su dati più chiari, ricostruzioni più precise e responsabilità meglio individuabili.

Accanto a questi indubbi punti di forza, emergono però debolezze strutturali

che non dipendono dalla tecnologia, ma dal contesto organizzativo in cui essa viene inserita. In molti uffici della Pubblica Amministrazione, l'innovazione digitale convive con pratiche amministrative superate, generando duplicazioni di passaggi, un appesantimento dei carichi di lavoro e una confusione di ruoli e responsabilità. Piattaforme informatiche non dialoganti tra loro, sistemi utilizzati solo in minima parte delle loro potenzialità e procedure digitali affiancate da archivi cartacei sono segnali evidenti di una trasformazione incompleta, spesso subita più che governata.

Uno degli elementi più critici che emergono nell'esperienza dell'Ombudsman è rappresentato dalle sacche di resistenza interna presenti in molti uffici della Pubblica Amministrazione. Si tratta di resistenze raramente esplicite, ma profondamente radicate, che si manifestano attraverso inerzia, rigidità interpretativa e un uso difensivo delle regole e delle procedure. In questo contesto, la tecnologia può diventare una vera e propria zavorra: anziché favorire il cambiamento, viene utilizzata come giustificazione per non decidere, per rinviare o per negare soluzioni ragionevoli ai cittadini.

Non è raro che l'amministrazione attribuisca al sistema informatico la responsabilità di ritardi o dinieghi, come se l'algoritmo o la piattaforma fossero entità autonome e incontestabili. Espressioni come "il sistema non lo consente" o "la procedura non prevede alternative" diventano formule di deresponsabilizzazione, dietro le quali si nasconde spesso la rinuncia a esercitare un margine di valutazione e di buon senso. In questi casi, la tecnologia non solo non migliora il rapporto con il cittadino, ma contribuisce a renderlo più distante e conflittuale.

Un esempio emblematico riguarda la gestione delle istanze digitali che presentano errori formali minimi o facilmente sanabili. In alcuni uffici, l'impossibilità di intervenire sul sistema informatico viene utilizzata come motivo per rigettare la domanda, senza considerare la sostanza della richiesta e senza offrire al cittadino un supporto concreto per correggere l'errore. In tali circostanze, la tecnologia diventa un ostacolo e il principio di buon andamento dell'amministrazione risulta gravemente compromesso.

Le raccomandazioni dell'Ombudsman, in questi contesti, assumono un valore che va oltre la risoluzione del singolo caso. Esse possono e devono indicare la necessità di superare un approccio meramente formale all'innovazione, sollecitando un uso delle tecnologie coerente con la finalità pubblica dell'azione amministrativa. Raccomandare significa anche richiamare l'amministrazione alla responsabilità, ricordando che nessun sistema informatico può sostituire completamente il giudizio umano e che la tecnologia deve restare uno strumento al servizio delle persone, e non il contrario.

Il nodo centrale resta, dunque, culturale. Senza un cambiamento profondo nel modo di concepire il lavoro pubblico, ogni innovazione rischia di essere assorbita e neutralizzata dalle stesse dinamiche che avrebbe dovuto superare. Le nuove tecnologie possono rafforzare l'efficienza, la trasparenza e l'equità solo se inserite in un contesto che valorizzi la responsabilità individuale, la formazione continua e l'orientamento al servizio.

In questo scenario, l'Ombudsman può svolgere un ruolo decisivo quale figura di equilibrio e di stimolo, capace di leggere le criticità sistemiche e di utilizzare le raccomandazioni come leva per un cambiamento reale. Superare la zavorra delle resistenze interne significa restituire alla Pubblica Amministrazione la capacità di muoversi con maggiore agilità, rispondere in modo più efficace ai bisogni dei cittadini e utilizzare le tecnologie per ciò che realmente sono: strumenti per migliorare la qualità della democrazia amministrativa.

Capitolo 3

USO DELLE NUOVE TECNOLOGIE NELLA PROMOZIONE E NELL'EDUCAZIONE AI DIRITTI UMANI NEL CONTESTO MESSICANO

(Ignacio Domínguez)

Nel contesto internazionale attuale, la promozione e l'educazione ai diritti umani non possono più dipendere esclusivamente da metodi tradizionali. La trasformazione digitale ha ridefinito il modo in cui le società apprendono, si informano e partecipano. Oggi l'intelligenza artificiale, le piattaforme digitali, l'analisi dei dati e il marketing digitale strategico sono diventati strumenti chiave per ampliare la portata, l'accessibilità e l'impatto dei programmi educativi sui diritti umani a livello globale.

Da una prospettiva lungimirante — particolarmente rilevante per leader accademici, consulenti e responsabili delle politiche pubbliche — le nuove tecnologie non sostituiscono l'approccio umanistico: lo potenziano, lo ottimizzano e lo rendono misurabile.

1. L'intelligenza artificiale come motore dell'educazione personalizzata sui diritti umani

L'intelligenza artificiale ha consentito di progettare modelli educativi adattivi, capaci di analizzare il comportamento dell'utente e di adeguare i contenuti al suo livello di comprensione, alla lingua, al contesto culturale e alle necessità specifiche.

A livello internazionale, organismi multilaterali e università hanno implementato piattaforme di formazione basate sull'IA per preparare funzionari pubblici in materia di diritti fondamentali, prevenzione della discriminazione e accesso alla giustizia. Questi sistemi utilizzano l'analisi dell'apprendimento per rilevare lacune formative e raccomandare percorsi educativi personalizzati, aumentando l'efficacia pedagogica.

Per esempio, simulatori basati sull'IA sono stati utilizzati nella formazione dei corpi di sicurezza e degli operatori giuridici, ricreando scenari relativi all'uso legittimo della forza, al giusto processo e alla protezione dei diritti umani, così da rafforzare il processo decisionale secondo un approccio etico e normativo.

2. Marketing digitale con approccio sociale: visibilità e sensibilizzazione strategica

Il marketing digitale si è consolidato come strumento di grande impatto per la promozione dei diritti umani. Attraverso campagne segmentate, contenuti audiovisivi, storytelling sociale e strategie di posizionamento digitale, le istituzioni riescono a sensibilizzare gruppi specifici di popolazione con messaggi chiari ed emotivamente rilevanti.

Campagne digitali su uguaglianza, inclusione, diritti dell'infanzia e non discriminazione hanno raggiunto milioni di persone tramite i social network, dimostrando che l'educazione ai diritti umani, quando comunicata con tecniche di marketing digitale, genera maggiore comprensione, partecipazione civica e consapevolezza collettiva.

3. Piattaforme digitali ed educazione aperta: accesso senza frontiere

Le aule virtuali, i corsi online e i webinar specialistici hanno rivoluzionato l'educazione ai diritti umani, eliminando barriere geografiche ed economiche.

Attualmente, migliaia di funzionari pubblici, accademici, studenti e difensori dei diritti accedono a contenuti certificati su trattati internazionali, giurisprudenza in materia di diritti umani e governance democratica tramite piattaforme digitali dotate di valutazioni automatizzate e monitoraggio formativo.

4. Big Data e analisi predittiva per politiche educative sui diritti umani

L'uso dell'analisi dei dati permette di identificare schemi di violazione dei diritti e di progettare strategie educative mirate. Dashboard intelligenti consentono alle istituzioni di visualizzare indicatori relativi a violenza, discriminazione, esclusione sociale e accesso alla giustizia, facilitando decisioni basate sull'evidenza.

Nei contesti di crisi sociale, il monitoraggio digitale delle tendenze informative è stato utilizzato per rilevare discorsi d'odio e progettare campagne educative preventive orientate alla cultura della pace e della legalità.

5. Tecnologie immersive ed educazione esperienziale

La realtà virtuale e le tecnologie immersive hanno introdotto un approccio pedagogico innovativo: apprendere i diritti umani attraverso l'esperienza.

Le simulazioni digitali permettono di comprendere situazioni di sfollamento, discriminazione o violazione dei diritti da una prospettiva empatica, rafforzando la sensibilizzazione istituzionale e sociale.

6. Esempio reale nel contesto dei diritti umani in Messico

In Messico, un caso rilevante è rappresentato dalla digitalizzazione dei programmi educativi e delle campagne di promozione dei diritti umani promosse da istituzioni quali le commissioni per i diritti umani e gli organismi accademici, che hanno integrato piattaforme virtuali, social network e strumenti digitali per la formazione cittadina.

Ad esempio, negli ultimi anni diverse istituzioni pubbliche hanno implementato corsi online di massa su diritti umani, prospettiva di genere e diritti dei gruppi vulnerabili, rivolti a funzionari pubblici, studenti e cittadini in generale. Questi programmi digitali hanno ampliato significativamente la portata educativa, passando da formazioni in presenza, necessariamente limitate, a percorsi capaci di coinvolgere simultaneamente migliaia di partecipanti in tutto il Paese.

Allo stesso modo, l'uso dei social network e di campagne digitali istituzionali è stato fondamentale per promuovere la cultura dei diritti umani su temi quali la prevenzione della violenza, i diritti dell'infanzia, i diritti delle donne e l'accesso alla giustizia. Attraverso infografiche, capsule educative, webinar e contenuti interattivi, è stato possibile sensibilizzare la popolazione giovane, segmento altamente digitalizzato.

Un caso particolarmente strategico è costituito dall'uso di piattaforme tecnologiche per la ricezione di denunce online e per l'orientamento digitale in materia di diritti umani, riducendo le barriere di accesso alla giustizia, soprattutto per le popolazioni vulnerabili che vivono in aree rurali o che presentano limitazioni di mobilità. Questa trasformazione digitale rafforza il principio di accessibilità, uno dei pilastri del sistema internazionale dei diritti umani.

7. Rischi etici e governance tecnologica nei diritti umani

L'integrazione tecnologica deve essere allineata ai principi di etica digitale, protezione dei dati personali, trasparenza algoritmica e non discriminazione. In contesti come il Messico e l'America Latina, nei quali il divario digitale rappresenta ancora un fattore critico, l'implementazione delle tecnologie nell'ambito dei diritti umani deve essere inclusiva, interculturale e regolatoriamente solida.

Le istituzioni devono garantire che l'intelligenza artificiale e i sistemi digitali rispettino la dignità umana, evitino bias algoritmici e siano conformi agli standard internazionali in materia di diritti umani e governance tecnologica.

Conclusione strategica e motivazionale

La promozione e l'educazione ai diritti umani stanno entrando in una nuova era: digitale, intelligente e strategica. In Paesi come il Messico, dove le sfide sociali coesistono con una crescente trasformazione tecnologica, l'uso dell'intelligenza artificiale, delle piattaforme educative digitali e del marketing sociale rappresenta un'opportunità storica per rafforzare la cultura della legalità e il rispetto dei diritti fondamentali.

La tecnologia, quando implementata con visione etica, approccio pedagogico e leadership istituzionale, non solo educa: potenzia, previene violazioni e costruisce società più consapevoli, inclusive e resilienti. Nel XXI secolo, la difesa dei diritti umani si svolge anche nell'ambiente digitale, e chi saprà governare questi strumenti guiderà la trasformazione educativa e sociale del futuro.

Capitolo 4

PROTEZIONE DEI GRUPPI VULNERABILI

(Ignacio Domínguez)

Approccio strategico con applicazioni dell'Intelligenza Artificiale e relativo impatto positivo

La protezione dei gruppi vulnerabili costituisce uno dei pilastri fondamentali del sistema internazionale dei diritti umani. Nel contesto messicano, caratterizzato dalla compresenza di sfide sociali complesse — quali disuguaglianza strutturale, divario digitale, violenza di genere, fenomeni migratori ed esclusione economica — l'uso dell'intelligenza artificiale (IA) si configura come uno strumento potenzialmente trasformativo per rafforzare la prevenzione, l'assistenza, l'educazione e la tutela effettiva dei diritti umani.

In una prospettiva contemporanea e orientata al futuro, l'intelligenza artificiale non sostituisce l'intervento istituzionale né l'approccio umanistico, ma li potenzia, rendendoli più efficaci attraverso l'analisi predittiva, l'automazione responsabile, l'accessibilità digitale e l'assunzione di decisioni basate su dati ed evidenze.

1. Protezione dell'infanzia e dell'adolescenza negli ambienti digitali

L'infanzia rappresenta uno dei gruppi maggiormente esposti a rischi quali violenza digitale, sfruttamento, abbandono scolastico e cyberbullismo. In tale ambito, l'intelligenza artificiale consente di monitorare situazioni di rischio, prevenire violazioni e progettare interventi educativi personalizzati secondo un approccio fondato sui diritti umani.

Esempio applicativo in Messico (IA e diritti dell'infanzia):

Nel sistema educativo messicano, piattaforme digitali basate sull'IA possono analizzare indicatori quali assenteismo scolastico, rendimento accademico e comportamento online, al fine di individuare precocemente situazioni di rischio, come l'abbandono scolastico o contesti di violenza domestica.

Ad esempio, un sistema di analisi predittiva implementato nelle scuole pubbliche potrebbe rilevare variazioni significative nel rendimento e nella frequenza di un minore, attivando automaticamente l'intervento di orientatori scolastici e assistenti sociali, secondo un approccio di protezione integrata.

Impatto positivo:

• prevenzione precoce delle violazioni dei diritti dell'infanzia;

• riduzione dell'abbandono scolastico;

• interventi mirati nei confronti dei minori in situazione di rischio;

• rafforzamento del diritto all'educazione e allo sviluppo integrale.

2. Protezione delle donne e prevenzione della violenza di genere

La violenza contro le donne costituisce una problematica strutturale nel contesto messicano. L'intelligenza artificiale offre strumenti utili per analizzare pattern di violenza, migliorare i meccanismi di segnalazione e rafforzare le politiche pubbliche di prevenzione.

Esempio applicativo in Messico (IA e protezione delle donne):

L'impiego di sistemi di IA nelle piattaforme digitali di denuncia consente di analizzare linguaggio, frequenza delle segnalazioni e localizzazione geografica, al fine di individuare aree ad alto rischio di violenza di genere.

Ad esempio, un'applicazione istituzionale può classificare automaticamente le segnalazioni relative a violenza domestica, rischio di femminicidio o molestie, attribuendo priorità ai casi più urgenti e favorendo un intervento tempestivo da parte delle autorità e degli organismi di tutela dei diritti umani.

Impatto positivo:

• maggiore tempestività ed efficienza della risposta istituzionale;

• prioritarizzazione dei casi più gravi;

• riduzione della vittimizzazione secondaria;

• rafforzamento dell'accesso alla giustizia in un'ottica di genere.

3. Protezione delle persone migranti e rifugiate

Il Messico, quale Paese di transito e destinazione migratoria, affronta sfide rilevanti nella tutela dei diritti delle persone migranti, spesso esposte a discriminazione, violenza ed esclusione sociale.

Esempio applicativo in Messico (IA e diritti dei migranti):

Sistemi di intelligenza artificiale possono essere integrati in piattaforme digitali multilingue, in grado di fornire informazioni automatizzate su diritti, servizi legali, assistenza sanitaria e procedure di protezione.

Un assistente virtuale accessibile tramite dispositivi mobili può offrire supporto in tempo reale in diverse lingue - tra cui spagnolo, inglese e lingue indigene - informando i migranti sui loro diritti, sui percorsi sicuri e sui meccanismi di denuncia disponibili.

Impatto positivo:

• accesso immediato alle informazioni sui diritti umani;

• riduzione della disinformazione e della vulnerabilità;

• inclusione linguistica e culturale;

• tutela della dignità e della sicurezza personale.

4. Protezione delle persone con disabilità e accessibilità tecnologica

Le persone con disabilità incontrano ancora significative barriere nell'accesso all'istruzione, al lavoro, alla giustizia e ai servizi pubblici. L'intelligenza artificia-

le consente di sviluppare soluzioni inclusive e accessibili, in linea con i principi di uguaglianza e non discriminazione.

Esempio applicativo in Messico (IA, inclusione e disabilità):

L'utilizzo di sistemi di riconoscimento vocale, sottotitolazione automatica e assistenti virtuali accessibili nelle piattaforme istituzionali consente alle persone con disabilità sensoriali di accedere più agevolmente alle informazioni pubbliche.

Ad esempio, i portali digitali delle istituzioni possono integrare strumenti di traduzione automatica in linguaggio semplificato, audiodescrizioni e contenuti in Lingua dei Segni Messicana tramite avatar digitali.

Impatto positivo:

• accesso equo all'informazione pubblica;

• inclusione digitale effettiva;

• rafforzamento del principio di uguaglianza;

• riduzione delle barriere tecnologiche.

5. Protezione delle comunità indigene e riduzione del divario digitale

Le comunità indigene in Messico costituiscono un gruppo particolarmente vulnerabile a causa di disuguaglianze storiche, limitato accesso ai servizi e barriere linguistiche.

Esempio applicativo in Messico (IA e diritti dei popoli indigeni):

L'intelligenza artificiale può essere impiegata in piattaforme educative interculturali capaci di tradurre automaticamente contenuti sui diritti umani nelle lingue indigene, quali náhuatl, maya, mixteco e zapoteco.

Inoltre, sistemi di analisi dei dati possono individuare aree di maggiore vulnerabilità, consentendo di indirizzare in modo più efficace programmi educativi e interventi di protezione sociale.

Impatto positivo:

• educazione ai diritti umani culturalmente pertinente;

• riduzione dell'esclusione linguistica;

• valorizzazione dell'identità culturale;

• maggiore efficacia delle politiche pubbliche inclusive.

6. Protezione degli anziani in contesti di vulnerabilità sociale

L'invecchiamento della popolazione richiede strategie innovative per garantire diritti fondamentali quali salute, sicurezza e accesso ai servizi.

Esempio applicativo in Messico (IA e diritti degli anziani):

Sistemi di monitoraggio intelligente integrati nei programmi sociali possono individuare situazioni di isolamento, mancato accesso ai servizi sanitari o rischio di esclusione economica.

Ad esempio, una piattaforma basata su IA può segnalare alle istituzioni la mancata fruizione di servizi medici da parte di un anziano, attivando interventi di supporto mirati.

Impatto positivo:

• prevenzione dell'abbandono e dell'isolamento sociale;

• miglioramento dell'assistenza sanitaria preventiva;

• tutela del diritto a una vita dignitosa;

• ottimizzazione dei programmi sociali.

7. Governance etica dell'intelligenza artificiale

L'impiego dell'intelligenza artificiale nella tutela dei diritti umani deve essere guidato da principi di legalità, trasparenza, protezione dei dati personali e non discriminazione. Nel contesto messicano, ciò implica l'allineamento delle soluzioni tecnologiche ai quadri normativi nazionali e agli standard internazionali.

Esempio applicativo in Messico (IA etica e diritti umani):

L'adozione di algoritmi verificabili nei sistemi di assegnazione degli aiuti sociali può contribuire a prevenire bias discriminatori e a garantire una distribuzione equa delle risorse, basata su criteri oggettivi.

Impatto positivo:

• maggiore equità e trasparenza nelle decisioni;

• riduzione dei bias istituzionali;

• rafforzamento della fiducia pubblica;

• tutela integrale dei diritti nell'ambiente digitale.

Conclusione strategica

La protezione dei gruppi vulnerabili in Messico richiede un'evoluzione istituzionale fondata sull'integrazione tra tecnologia, etica e diritti umani. L'intelligenza artificiale, se utilizzata in modo responsabile e strategico, consente di anticipare i rischi, ampliare l'accesso alla giustizia, personalizzare gli interventi educativi e rafforzare l'inclusione sociale.

L'impatto positivo è evidente: maggiore efficienza istituzionale, riduzione delle disuguaglianze e tutela più efficace della dignità umana. Nel XXI secolo, la vera innovazione non si misura soltanto nel progresso tecnologico, ma nella capacità

di proteggere chi si trova in condizioni di maggiore vulnerabilità. In questa prospettiva, l'intelligenza artificiale, guidata da un approccio umanistico, si configura come uno strumento essenziale per la costruzione di una società più giusta, inclusiva e resiliente.

Capitolo 5

USO DELLE NUOVE TECNOLOGIE NELLA CONSULENZA E NELL'ACCOMPAGNAMENTO DELLE VITTIME

(Ignacio Domínguez)

Approccio strategico con l'Intelligenza Artificiale e relativo impatto positivo in contesti critici

La consulenza e l'accompagnamento delle vittime costituiscono funzioni essenziali all'interno del sistema di tutela dei diritti umani, in particolare in contesti critici quali la violenza di genere, le violazioni dei diritti fondamentali, lo sfollamento, i reati, l'abuso istituzionale e le crisi umanitarie. Nell'era digitale, le nuove tecnologie — in particolare l'intelligenza artificiale (IA), le piattaforme digitali, l'analisi dei dati e i sistemi automatizzati di assistenza — stanno ridefinendo le modalità attraverso cui le istituzioni forniscono orientamento, supporto psicologico, consulenza giuridica e monitoraggio integrato delle vittime.

In una prospettiva al tempo stesso tecnica e umanistica, la tecnologia non sostituisce l'accompagnamento umano, ma lo rafforza, rendendolo più accessibile, tempestivo, scalabile e centrato sulla dignità della persona, riducendo le barriere di accesso alla giustizia e ai servizi di protezione.

1. Consulenza legale digitale assistita da intelligenza artificiale

L'accesso alla consulenza legale rappresenta una delle principali barriere per le vittime, soprattutto in contesti di vulnerabilità economica, geografica o sociale. L'intelligenza artificiale consente di automatizzare l'orientamento giuridico iniziale, l'analisi dei casi e l'individuazione delle possibili azioni istituzionali.

Esempio applicativo (IA nella consulenza legale per vittime di violazioni dei diritti umani):

Una piattaforma istituzionale basata su IA può operare come assistente legale digitale che, attraverso tecniche di elaborazione del linguaggio naturale, analizza il racconto della vittima (denuncia, reclamo o testimonianza) e classifica la tipologia di violazione (discriminazione, abuso di autorità, violenza, omissione istituzionale).

Il sistema è in grado di suggerire percorsi giuridici, indicare le autorità competenti, segnalare termini rilevanti e individuare i diritti applicabili, in conformità al quadro normativo nazionale e internazionale.

Impatto positivo in contesti critici:

• accesso immediato all'orientamento legale, senza barriere geografiche;

• riduzione dei tempi di risposta istituzionale;

• rafforzamento dell'autonomia giuridica della vittima;

• maggiore effettività del diritto di accesso alla giustizia.

2. Accompagnamento psicologico digitale e assistenza emotiva con IA

Le vittime di violenza, abuso o crisi umanitarie necessitano di un supporto emotivo continuo e qualificato. Le tecnologie basate su IA consentono di sviluppare sistemi di assistenza psicologica digitale accessibili e riservati.

Esempio applicativo (IA nel supporto emotivo alle vittime):

Un sistema di accompagnamento psicologico basato su IA può offrire assistenza iniziale continua (24/7) attraverso chatbot addestrati in tecniche di primo supporto psicologico, individuazione delle crisi emotive e orientamento verso specialisti umani.

L'IA può analizzare schemi linguistici per rilevare livelli di ansia, stress post-traumatico o rischio elevato, attivando segnalazioni automatiche per un intervento professionale tempestivo.

Impatto positivo in contesti critici:

• disponibilità immediata di supporto emotivo;

• riduzione dell'isolamento psicologico della vittima;

• individuazione precoce delle situazioni di crisi;

• tutela del diritto alla salute mentale e alla dignità personale.

3. Piattaforme digitali di denuncia e monitoraggio intelligente dei casi

Molte vittime non denunciano per timore, mancanza di informazioni o difficoltà di accesso ai canali istituzionali. Le nuove tecnologie consentono di realizzare sistemi digitali sicuri, anche anonimi, per la ricezione e la gestione delle segnalazioni.

Esempio applicativo (IA nei sistemi di denuncia digitale):

Una piattaforma di denuncia dotata di IA può ricevere segnalazioni online, verificarne la coerenza, valutarne l'urgenza e attribuire priorità automatica ai casi più gravi (ad esempio, situazioni di violenza estrema o rischio per la vita).

Il sistema può inoltre generare un fascicolo digitale tracciabile, con monitoraggio automatico e aggiornamenti sullo stato del procedimento, riducendo il rischio di rivittimizzazione istituzionale.

Impatto positivo in contesti critici:

• rafforzamento della fiducia nelle istituzioni;

• aumento delle denunce di violazioni dei diritti;

• maggiore trasparenza e tracciabilità dei procedimenti;

• riduzione della rivittimizzazione burocratica.

4. Accompagnamento integrato mediante analisi predittiva

L'intelligenza artificiale consente di individuare fattori di rischio e di progettare percorsi di accompagnamento personalizzati, in particolare in contesti di violenza domestica, tratta di persone o sfollamento forzato.

Esempio applicativo (IA nel monitoraggio integrato delle vittime):

Un sistema istituzionale può integrare dati sociali, psicologici e giuridici relativi ai singoli casi (nel rispetto dei principi di protezione dei dati) per elaborare profili di rischio e individuare bisogni specifici.

Ad esempio, nel caso di una vittima di violenza con precedenti episodi di recidiva dell'aggressore e condizioni di vulnerabilità economica, il sistema può

suggerire l'adozione di misure di protezione prioritarie, interventi di sostegno sociale e assistenza legale rafforzata.

Impatto positivo in contesti critici:

• protezione preventiva e personalizzata;

• riduzione del rischio di reiterazione della violenza;

• approccio integrato e multidisciplinare;

• maggiore efficacia delle politiche di protezione.

5. Accessibilità tecnologica per vittime in condizioni di vulnerabilità

Le vittime residenti in aree rurali, comunità indigene o contesti di esclusione sociale incontrano spesso ostacoli significativi nell'accesso ai servizi istituzionali. Le tecnologie digitali contribuiscono a ridurre tali barriere.

Esempio applicativo (IA multilingue e inclusiva):

Assistenti virtuali basati su IA possono offrire consulenza in più lingue, comprese le lingue indigene, attraverso interfacce accessibili da dispositivi mobili.

In tal modo, una vittima può ricevere informazioni sui propri diritti, sui meccanismi di denuncia e sui servizi disponibili senza necessità di spostamenti fisici.

Impatto positivo in contesti critici:

• inclusione linguistica e digitale;

• riduzione delle barriere territoriali;

• accesso equo ai servizi di protezione;

• rafforzamento del principio di non discriminazione.

6. Uso dell'intelligenza artificiale nella protezione delle vittime di violenza digitale

La violenza digitale, le molestie online e la diffusione illecita di contenuti rappresentano nuove forme di aggressione ai diritti della persona.

Esempio applicativo (IA nella protezione contro la violenza digitale):

Sistemi di IA possono monitorare ambienti digitali per individuare contenuti offensivi, minacce o diffusioni non autorizzate di dati personali, attivando procedure di segnalazione e rimozione.

Parallelamente, le piattaforme di accompagnamento possono offrire orientamento legale, supporto nella raccolta di prove digitali e assistenza nei percorsi di denuncia.

Impatto positivo in contesti critici:

• tutela dell'identità digitale;

• riduzione del danno psicologico e sociale;

• risposta tempestiva alle aggressioni online;

• rafforzamento del diritto alla privacy e alla sicurezza digitale.

7. Governance etica e protezione dei dati

L'impiego delle tecnologie nella consulenza e nell'accompagnamento delle vittime deve rispettare rigorosi principi di riservatezza, protezione dei dati personali, centralità della persona e trasparenza algoritmica.

Esempio applicativo (IA etica nella gestione dei casi):

Una piattaforma istituzionale basata su IA può integrare sistemi di anonimizzazione, crittografia dei dati e audit algoritmici, al fine di garantire la sicurezza delle informazioni e prevenire utilizzi impropri.

Tali misure risultano particolarmente rilevanti nei casi di violenza, abuso istituzionale o reati gravi, nei quali la protezione della vittima costituisce una priorità assoluta.

Impatto positivo in contesti critici:

• tutela integrale delle informazioni sensibili;

• rafforzamento della fiducia istituzionale;

• prevenzione di violazioni e fughe di dati;

• uso responsabile e conforme della tecnologia.

Conclusione strategica

L'impiego delle nuove tecnologie nella consulenza e nell'accompagnamento delle vittime rappresenta una trasformazione strutturale nei sistemi di tutela dei diritti umani. L'intelligenza artificiale consente di offrire interventi più rapidi, personalizzati e accessibili, soprattutto nei contesti critici in cui la tempestività e l'accuratezza dell'azione istituzionale risultano determinanti.

Se implementata secondo un approccio etico, giuridico e umanistico, la tecnologia si configura come uno strumento di giustizia, protezione ed empatia. Il suo impatto è rilevante: maggiore accesso alla giustizia, miglioramento del supporto emotivo, riduzione dei rischi e rafforzamento dell'efficacia istituzionale.

Nel prossimo futuro, i sistemi di accompagnamento che integrano l'intelligenza artificiale saranno sempre più capaci di garantire una tutela concreta, inclusiva e resiliente dei diritti umani.

Capitolo 6

I DIRITTI UMANI E IL CALCOLO QUANTISTICO

(Ignacio Domínguez)

Convergenza strategica tra Intelligenza Artificiale, calcolo quantistico e protezione della dignità umana

Il calcolo quantistico rappresenta una delle tecnologie emergenti con il maggiore potenziale trasformativo del XXI secolo. La sua capacità di elaborare informazioni attraverso qubit, sovrapposizione ed entanglement quantistico permette di affrontare problemi complessi con velocità e capacità di calcolo potenzialmente superiori rispetto alla computazione classica. Nell'ambito dei diritti umani, la sua integrazione con l'intelligenza artificiale apre un nuovo paradigma: sistemi predittivi, etici e altamente accurati per la protezione della dignità umana, della giustizia, dell'inclusione e della governance basata sull'evidenza.

In una prospettiva orientata al futuro, il calcolo quantistico non deve essere concepito soltanto come uno strumento tecnologico avanzato, ma come un abilitatore strategico per rafforzare i sistemi di protezione dei diritti umani in contesti complessi, critici e multidimensionali.

1. Protezione del diritto alla privacy e sicurezza dei dati

La privacy è un diritto umano fondamentale. Tuttavia, l'avanzamento del calcolo quantistico presenta rischi e opportunità in materia di cybersicurezza e protezione dei dati sensibili, soprattutto nelle banche dati delle vittime, degli organismi di tutela dei diritti umani e dei sistemi giudiziari.

Esempio applicativo: IA e calcolo quantistico nella protezione dei dati delle vittime

Un sistema istituzionale dedicato ai diritti umani può integrare l'IA per la gestione dei fascicoli digitali e, parallelamente, utilizzare algoritmi di crittografia post-quantistica resistenti ad attacchi quantistici, al fine di proteggere informazioni altamente sensibili, quali denunce, testimonianze e dati biometrici.

L'IA classifica e anonimizza le informazioni, mentre la cifratura post-quantistica rafforza la protezione dei dati rispetto alle minacce tecnologiche future.

Impatto positivo:

• protezione rafforzata del diritto alla privacy;

• sicurezza avanzata delle informazioni sensibili;

• prevenzione di fughe di dati e rivittimizzazione;

• maggiore fiducia nei sistemi digitali dedicati ai diritti umani.

2. Analisi predittiva delle violazioni dei diritti umani mediante IA quantistica

La prevenzione delle violazioni dei diritti umani richiede modelli analitici capaci di elaborare variabili sociali, economiche e territoriali complesse. La computazione quantistica, combinata con l'IA, può consentire di costruire scenari predittivi di maggiore ampiezza e precisione.

Esempio applicativo: IA quantistica nell'analisi dei rischi sociali

Un osservatorio dei diritti umani può utilizzare algoritmi di machine learning accelerati dal calcolo quantistico per analizzare grandi volumi di dati relativi a indicatori di violenza, disuguaglianza, migrazione, povertà e conflitti sociali.

Il sistema può così individuare schemi ricorrenti o difficilmente visibili con strumenti tradizionali, segnalando aree ad alto rischio di violazione dei diritti e consentendo interventi istituzionali preventivi e politiche pubbliche mirate.

Impatto positivo:

• prevenzione strutturale delle violazioni dei diritti umani;

• decisioni basate su evidenze avanzate;

• ottimizzazione delle politiche pubbliche sociali;

• protezione anticipata delle popolazioni vulnerabili.

3. Accesso alla giustizia e sistemi giudiziari intelligenti

L'accesso alla giustizia è un diritto essenziale che può essere rafforzato attraverso tecnologie avanzate capaci di ottimizzare l'analisi giuridica e la gestione di casi complessi.

Esempio applicativo: IA giuridica e calcolo quantistico

Un sistema giudiziario intelligente può utilizzare l'IA per analizzare giurisprudenza, trattati internazionali e precedenti giuridici, mentre il calcolo quantistico può contribuire all'ottimizzazione di problemi complessi attraverso simulazioni probabilistiche di scenari legali.

Ciò consentirebbe di attribuire priorità ai casi relativi a violazioni dei diritti umani, individuare schemi di impunità e ridurre i tempi procedurali nelle situazioni più critiche.

Impatto positivo:

• maggiore efficienza giudiziaria;

• riduzione dei ritardi procedurali;

• accesso più equo alla giustizia;

• rafforzamento dello Stato di diritto.

4. Protezione dei gruppi vulnerabili tramite simulazioni quantistiche sociali

Il calcolo quantistico può consentire la simulazione di sistemi sociali complessi, con potenziali ricadute nella progettazione di politiche pubbliche inclusive fondate su un approccio orientato ai diritti umani.

Esempio applicativo: IA e simulazione quantistica nelle politiche sociali

Un modello di simulazione quantistica può analizzare l'impatto di determinate politiche pubbliche su comunità vulnerabili - infanzia, donne, migranti o popoli indigeni - integrando variabili socioeconomiche, educative e territoriali.

L'IA può interpretare i risultati del modello e suggerire strategie di intervento

sociale finalizzate a ridurre le disuguaglianze strutturali.

Impatto positivo:

• progettazione di politiche pubbliche più giuste e inclusive;

• riduzione delle disuguaglianze sociali;

• protezione mirata dei gruppi vulnerabili;

• pianificazione strategica basata su scenari complessi.

5. Diritti umani, salute e medicina quantistica predittiva

Il diritto alla salute può essere rafforzato dalla convergenza tra IA e computazione quantistica, soprattutto nella prevenzione delle malattie e nell'ottimizzazione dei trattamenti.

Esempio applicativo: IA medica e calcolo quantistico

Sistemi di IA integrati con algoritmi quantistici possono analizzare ampie basi di dati biomedici per rilevare indicatori precoci di malattie nelle popolazioni vulnerabili.

Nel contesto della salute pubblica, il calcolo quantistico può contribuire a modellare la propagazione epidemiologica con maggiore precisione, favorendo strategie preventive e una distribuzione più efficiente delle risorse mediche.

Impatto positivo:

• rafforzamento del diritto alla salute;

• diagnosi precoce nelle popolazioni vulnerabili;

• ottimizzazione delle risorse sanitarie;

• riduzione dei rischi epidemiologici.

6. Educazione ai diritti umani mediante tecnologie quantistiche e IA

L'educazione è un diritto umano fondamentale e costituisce la base di società giuste e inclusive. La computazione quantistica può potenziare piattaforme educative intelligenti e altamente personalizzate.

Esempio applicativo: IA educativa e algoritmi quantistici

Piattaforme educative avanzate possono utilizzare l'IA per personalizzare contenuti sui diritti umani e algoritmi quantistici per ottimizzare modelli di apprendimento adattivo su larga scala.

Il sistema può analizzare stile cognitivo, contesto socioculturale e livello educativo dell'utente, offrendo percorsi formativi accessibili sui diritti umani.

Impatto positivo:

• democratizzazione della conoscenza sui diritti umani;

• educazione personalizzata e accessibile;

• riduzione delle disuguaglianze educative;

• rafforzamento della cultura della legalità.

7. Governance etica del calcolo quantistico e diritti umani

Lo sviluppo del calcolo quantistico deve essere allineato a principi etici, regolatori e di tutela dei diritti umani, al fine di prevenire rischi quali disuguaglianza tecnologica, sorveglianza eccessiva o concentrazione del potere tecnologico.

Esempio applicativo: IA etica e governance quantistica

Un quadro istituzionale può integrare sistemi di audit algoritmico basati su IA per supervisionare l'uso responsabile delle tecnologie quantistiche nelle politiche pubbliche, garantendo trasparenza, equità e rispetto dei diritti fondamentali.

Inoltre, modelli quantistici possono essere impiegati per valutare gli impatti normativi prima dell'implementazione di tecnologie dirompenti in settori sensibili.

Impatto positivo:

• uso responsabile ed etico delle tecnologie emergenti;

• prevenzione dei bias tecnologici;

• protezione delle libertà fondamentali;

• rafforzamento dei quadri regolatori in materia di diritti umani.

8. Cybersicurezza quantistica e protezione dei difensori dei diritti umani

I difensori dei diritti umani operano spesso in ambienti caratterizzati da elevati rischi digitali. Il calcolo quantistico applicato alla cybersicurezza può rafforzare la loro protezione tecnologica.

Esempio applicativo: IA e crittografia quantistica per la protezione degli attivisti

Sistemi di comunicazione cifrata, basati su tecniche resistenti alle minacce quantistiche, insieme al monitoraggio delle minacce mediante IA, possono proteggere le comunicazioni dei difensori dei diritti umani da attacchi informatici, spionaggio digitale o intercettazioni.

Impatto positivo:

• protezione della libertà di espressione;

• sicurezza digitale per difensori e organizzazioni;

• riduzione dei rischi di sorveglianza illegale;

• rafforzamento degli ecosistemi democratici.

Conclusione strategica e visione futura

La convergenza tra diritti umani, intelligenza artificiale e calcolo quantistico rappresenta un cambiamento paradigmatico nel modo in cui le istituzioni possono proteggere la dignità umana nell'era tecnologica. Queste tecnologie consentono di anticipare rischi, ottimizzare politiche pubbliche, rafforzare la

giustizia, proteggere dati sensibili e garantire diritti fondamentali con livelli di precisione sempre più elevati.

Lungi dall'essere necessariamente una minaccia, la computazione quantistica - se implementata con una governance etica e con un approccio umanistico - può diventare uno strumento strategico per la protezione integrale dei diritti umani. Il suo impatto positivo risiede nella capacità di affrontare problemi complessi, ridurre disuguaglianze strutturali e costruire sistemi istituzionali più intelligenti, resilienti e centrati sulla persona.

Nell'orizzonte del XXI secolo, la vera innovazione tecnologica sarà quella capace di porre i diritti umani al centro del proprio sviluppo quantistico e digitale.

Capitolo 7

Riflessioni conclusive

(Marino Fardelli)

Le considerazioni che emergono da questo lavoro conducono a una consapevolezza ulteriore rispetto a quella già maturata lungo il percorso argomentativo: la trasformazione in atto non è soltanto tecnologica, né esclusivamente organizzativa, ma propriamente istituzionale.

L'intelligenza artificiale, insieme alle altre tecnologie emergenti, non si limita a incidere sugli strumenti dell'azione amministrativa; essa interviene, più profondamente, sulle condizioni stesse di esercizio del potere pubblico. Cambiano le modalità di formazione delle decisioni, mutano i tempi e i luoghi della relazione tra cittadino e amministrazione, si ridefiniscono i confini tra discrezionalità e automatismo. In questo senso, la questione tecnologica si rivela, in ultima analisi, una questione di tenuta dell'ordinamento democratico.

In tale contesto, il ruolo del Difensore civico si colloca in una posizione peculiare e, per certi versi, privilegiata. Non essendo vincolato alle rigidità dell'azione amministrativa né alle forme del processo giurisdizionale, esso conserva quella flessibilità istituzionale che gli consente di intercettare precocemente le tensioni del sistema. Proprio questa caratteristica lo rende idoneo a svolgere una funzione che, oggi più che mai, appare essenziale: rendere visibile ciò che tende a diventare invisibile.

Se la burocrazia tradizionale era caratterizzata da un eccesso di formalismo, la burocrazia algoritmica rischia di produrre un effetto opposto ma altrettanto problematico: una semplificazione solo apparente, dietro la quale si celano processi decisionali complessi e difficilmente accessibili. Il cittadino non si confronta più con un atto percepito come distante, ma comprensibile; si confronta, sempre più spesso, con un esito che appare immediato ma opaco nelle sue determinanti.

È in questa tensione tra semplificazione e opacità che si inserisce la funzione della difesa civica. Non si tratta di opporsi all'innovazione, né di rallentarne il corso, ma di garantire che essa non produca una progressiva sottrazione di intelligibilità all'azione pubblica. In altri termini, il compito non è arrestare il cambiamento, ma ricondurlo entro coordinate di senso giuridico e democratico. Da questo punto di vista, la riflessione sull'intelligenza artificiale sollecita anche

una revisione del concetto stesso di responsabilità pubblica. Se, nel modello tradizionale, la responsabilità era prevalentemente legata all'atto finale, oggi essa tende a distribuirsi lungo l'intero ciclo di vita del dato e della decisione: dalla raccolta delle informazioni alla loro elaborazione, dalla configurazione degli algoritmi fino alla validazione dell'esito. La responsabilità diventa così diffusa, stratificata e organizzativa, richiedendo nuove forme di controllo e nuovi strumenti di garanzia.

In questo scenario, la difesa civica è chiamata a svolgere una funzione che potremmo definire di "ricomposizione": ricomporre la distanza tra decisione e comprensione, tra efficienza e giustizia, tra innovazione e diritti. È una funzione che non si esaurisce nell'intervento sul singolo caso, ma si estende alla capacità di leggere i fenomeni nella loro dimensione sistemica, individuando le criticità prima che esse si traducano in conflitti diffusi.

Accanto a questa dimensione istituzionale, emerge con forza anche una dimensione culturale. L'integrazione dell'intelligenza artificiale nella pubblica amministrazione non è soltanto una questione di norme o di tecnologie, ma di consapevolezza collettiva. Senza una adeguata comprensione dei meccanismi sottesi ai sistemi digitali, il rischio è quello di una delega inconsapevole, nella quale l'apparente neutralità della macchina finisce per sostituire il giudizio critico umano.

Per questo motivo, la sfida non riguarda solo i funzionari pubblici o gli operatori del diritto, ma l'intero corpo sociale. La tutela dei diritti nell'era digitale presuppone cittadini informati, istituzioni trasparenti e una cultura amministrativa capace di interrogare la tecnologia, senza subirla.

Guardando al futuro, appare evidente che il tema centrale non sarà tanto l'introduzione di nuove tecnologie, quanto la capacità delle istituzioni di governarne l'impatto nel tempo. L'evoluzione dell'intelligenza artificiale, e ancor più quella del calcolo quantistico, è destinata ad accelerare ulteriormente la complessità dei sistemi decisionali. In tale prospettiva, il rischio non è rappresentato da una singola tecnologia, ma dalla progressiva perdita di controllo sui processi che essa genera.

È qui che si misura, in ultima istanza, la funzione del Difensore civico: non soltanto come presidio di tutela, ma come custode dell'equilibrio tra innovazione e diritti. Un equilibrio che non può essere dato una volta per tutte, ma che deve essere costantemente ricercato, adattato e verificato alla luce dei mutamenti in atto.

Le pagine che precedono hanno mostrato come sia possibile immaginare un

modello di difesa civica capace di accompagnare la transizione digitale senza rinunciare ai propri principi fondativi. Le presenti riflessioni conclusive intendono ribadire un punto essenziale: il futuro dei diritti non dipenderà dalla tecnologia in sé, ma dalla qualità delle istituzioni chiamate a governarla.

In questo senso, il Difensore civico è destinato a rimanere una figura centrale. Non perché immune dal cambiamento, ma proprio perché capace di attraversarlo, mantenendo ferma la propria funzione originaria: garantire che, anche nell'era dell'algoritmo, la persona resti il punto di riferimento ultimo dell'azione pubblica.

El Defensor del Pueblo en la Era de la Inteligencia Artificial

Derechos y tecnologías emergentes: un enfoque estratégico, predictivo y transformador para la protección de los derechos.

Marino Fardelli

Defensor del Pueblo de la Región del Lacio
Presidente de la Coordinación Nacional de Defensores del Pueblo Italiano

Guido Giusti

Defensor del Pueblo de la Región Emilia-Romaña
Vicepresidente de la Coordinación Nacional de Defensores del Pueblo Italiano

Ignacio Domínguez

Director y CEO de Yakatiak, Consultores y Asociados. - México
Inteligencia Artificial, Cómputo Cuántico y Ciberseguridad

Índice

Introducción

Reflexiones de un Defensor Cívico

(Marino Fardelli)

Escribir hoy sobre inteligencia artificial, derechos y tecnologías emergentes desde la perspectiva de un defensor del pueblo implica asumir una responsabilidad que trasciende los límites del análisis institucional en sentido estricto. Significa, más profundamente, cuestionar el significado y la función del rol de garante en un momento histórico caracterizado por una clara discrepancia entre la velocidad del progreso tecnológico y la capacidad del sistema jurídico —así como de las propias instituciones y comunidades— para comprenderlo, gobernarlo y orientarlo. Es una responsabilidad que se sitúa en la intersección del derecho, la ética pública y la gobernanza de la innovación.

El defensor del pueblo nació como una autoridad local: escucha, media, protege y restablece el equilibrio. Su legitimidad se ha construido gradualmente sobre su relación directa con la ciudadanía, sobre su capacidad para restablecer el equilibrio y la humanidad allí donde la burocracia corre el riesgo de convertirse en distancia y los procedimientos administrativos en un mecanismo autorreferencial, potencialmente desconectado del individuo. Sin embargo, en el contexto tecnológico actual, esta función ya no puede limitarse a una lógica meramente reactiva, restringida a la intervención posterior a un daño ya producido.

La llegada de la inteligencia artificial, el desarrollo de la computación cuántica y la creciente importancia de la ciberseguridad exigen un cambio de paradigma: pasar de un modelo de protección basado en la respuesta a conflictos a uno orientado a la prevención, la anticipación y la gestión de riesgos sistémicos. Desde esta perspectiva, el Defensor del Pueblo está llamado a evolucionar hacia un rol estratégico y predictivo, capaz de identificar precozmente los problemas críticos generados por el uso de la tecnología y contribuir a la construcción de un ecosistema administrativo más equitativo, transparente y resiliente.

No se trata simplemente de resolver disputas individuales, sino de supervisar fenómenos complejos: prevenir nuevas formas de desigualdad digital, contrarrestar las dinámicas discriminatorias generadas por sistemas algorítmicos opacos y monitorear posibles vulneraciones silenciosas de los derechos fundamentales. La asimetría de información entre la administración y la ciudadanía, ya significativa en contextos tradicionales, corre el riesgo de verse aún más amplificada en presencia de sistemas automatizados de toma de decisiones, en los que

la opacidad técnica puede traducirse en opacidad jurídica.

Las tecnologías emergentes están transformando profundamente la relación entre la ciudadanía y la administración pública, entre los individuos y el poder de decisión, entre la libertad y el control. Algoritmos que asignan puntuaciones o prioridades, sistemas automatizados que guían las decisiones públicas, infraestructuras digitales que concentran y procesan enormes cantidades de datos personales y no personales: todo esto amplía significativamente la capacidad de acción de la administración, pero al mismo tiempo aumenta sus áreas de vulnerabilidad. El riesgo no reside únicamente en el error, sino también en que las decisiones sean prácticamente irrefutables cuando se basan en lógicas que no son del todo comprensibles ni verificables.

En este contexto, el Defensor del Pueblo no puede limitarse a un papel de observador. Se le exige que actúe como intérprete cualificado del cambio, garante de la transparencia y la explicabilidad algorítmica, guardián de la equidad digital y defensor de los derechos en el ecosistema tecnológico. Esto implica también el fortalecimiento de competencias: Junto con los conocimientos jurídicos tradicionales, resulta esencial una alfabetización tecnológica adecuada, capaz de comprender —al menos en sus aspectos fundamentales— la lógica operativa de los sistemas digitales.

Junto a esta dimensión institucional, surge inevitablemente una reflexión personal. Jamás habría imaginado que, tras presentar una tesis titulada “Servicios Telemáticos en Educación y Formación”, me encontraría, más de veintiséis años después, abordando la relación entre derechos y tecnología desde una perspectiva institucional. En aquel entonces, los servicios de telecomunicaciones representaban una promesa: Conexiones lentas, herramientas aún incipientes, una visión del futuro más posible que real.

Hoy, ese futuro se ha materializado plenamente, a menudo de maneras inesperadas. El progreso tecnológico ya no es simplemente un motor de oportunidades, sino que también es intrínsecamente ambivalente, exigiendo responsabilidad, gobernanza y una amplia concienciación. Si bien, por un lado, permite una mayor eficiencia, accesibilidad y calidad de los servicios públicos, por otro, plantea interrogantes sin precedentes sobre la protección de los derechos, el control democrático y la rendición de cuentas de las decisiones automatizadas.

Al observar el pasado y el presente, la rapidez del cambio resulta sin duda impactante. Pero aún más llamativa es la permanencia de ciertos elementos fundamentales: La necesidad de proteger al individuo, la centralidad de la dignidad humana y la necesidad de instituciones capaces de abordar las vulnerabilidades y garantizar la efectividad de los derechos. Los contextos, las herramientas y los

lenguajes cambian; sin embargo, los derechos siguen siendo el punto de referencia esencial en torno al cual debe girar la acción pública.

Este trabajo surge precisamente de esta convicción: La innovación tecnológica no es neutral y, en ausencia de una gobernanza orientada a los derechos, corre el riesgo de amplificar los desequilibrios existentes o generar otros nuevos. Desde esta perspectiva, el Defensor del Pueblo, en el horizonte 2026-2030, está llamado a posicionarse en un espacio sin precedentes, en el que la pericia jurídica, la sensibilidad social y el conocimiento tecnológico deben integrarse de manera estructural y continua.

La inteligencia artificial, la computación cuántica y la ciberseguridad no son ajenas a la figura del defensor del pueblo de hecho, constituyen nuevos ámbitos donde se desarrollará la protección concreta y efectiva de los derechos de los ciudadanos. Es en estos espacios donde se definirá la capacidad de las instituciones para mantenerse fieles a los principios de legalidad, imparcialidad y buen funcionamiento, incluso ante procesos de toma de decisiones cada vez más complejos y mediados por la tecnología.

Estas páginas no pretenden ofrecer soluciones definitivas ni un análisis exhaustivo de temas en constante evolución. Su objetivo, de forma más modesta pero no menos ambiciosa, es suscitar la reflexión, estimular el debate y esbozar un posible camino, el de un defensor del pueblo capaz no de perseguir la innovación, sino de acompañarla, guiarla y, cuando sea necesario, someterla a un riguroso escrutinio crítico.

El futuro de los derechos no se construye oponiéndose a la tecnología, sino gobernando con inteligencia, responsabilidad y visión. Esto significa apoyar los procesos innovadores sin estar sometido a ellos, prevenir la aparición de nuevas formas de desigualdad y promover un modelo de desarrollo tecnológico inclusivo, justo e informado, en consonancia con los principios fundamentales del ordenamiento jurídico.

Para fundamentar esta reflexión, este trabajo se enriquece con las valiosas contribuciones legales y técnicas de mis colegas, el abogado Guido Giusti y el Dr. Ignacio Domínguez. Nos conocimos durante una sesión de trabajo sobre buenas prácticas en una conferencia internacional de Defensores del Pueblo, y tuve la oportunidad de observar de primera mano cómo el valor de las relaciones profesionales se traduce en una capacidad eficaz para conectar diversas experiencias, habilidades y perspectivas.

En un contexto caracterizado por desafíos globales e interconectados, la colaboración entre abogados, técnicos e instituciones no es un elemento secundario, sino una condición esencial para la gestión de los procesos en curso. Es precisa-

mente a través de estas sinergias que se hace posible transformar la complejidad en oportunidad y convertir la cooperación en una herramienta concreta para la protección de los derechos en la era de las tecnologías emergentes.

PRIMERA PARTE

Defensa cívica, transparencia y gobernanza algorítmica.

LA EXPERIENCIA ITALIANA.

Capítulo 1

LA INTELIGENCIA ARTIFICIAL Y LA ADMINISTRACIÓN PÚBLICA.

(Guido Giusti)

De la práctica espontánea a la gobernanza del sistema.

La inteligencia artificial ya no es una frontera tecnológica por explorar, sino una realidad ineludible que la administración pública debe afrontar.

Como suele ocurrir con los procesos de innovación, en Italia el fenómeno precedió a su regulación. El uso de la Inteligencia Artificial ("IA") se infiltró en el trabajo diario de las oficinas públicas mucho antes de que la institución fuera plenamente consciente de sus implicaciones legales y organizativas.

Precisamente esta brecha entre la realidad y la planificación constituye el tema central de este artículo. No se trata de si la IA debe entrar en la administración pública, sino de si la administración es capaz de gestionar una tecnología que ya la impregna, impactando en los plazos, el lenguaje, las responsabilidades y las relaciones con los ciudadanos.

En todas las oficinas públicas, como en cualquier entorno profesional, los empleados ya utilizan herramientas de inteligencia artificial para redactar textos, resumir documentos, traducir comunicaciones y organizar información. Este uso suele ser individual, informal y, a veces, invisible para la organización.

Cuando este comportamiento se intensifica hasta convertirse en un uso verdaderamente indiscriminado, los expertos del sector lo denominan "IA en la sombra" (Shadow AI), un fenómeno ya generalizado en entornos corporativos e institucionales. Incluso cuando las organizaciones prohíben (o incluso bloquean) las principales aplicaciones de IA generativa, como ChatGPT, Gemini, Claude o Copilot, los empleados eluden el cortafuegos corporativo utilizando estas herramientas en sus dispositivos personales. La empresa, por supuesto, es incapaz de prevenir o supervisar este comportamiento, lo que provoca que el problema de seguridad que intentaba mitigar (en particular, la exposición involuntaria de datos confidenciales a entornos no autorizados) se agrave hasta el punto de descontrolarse.

Fuentes fiables describen un crecimiento significativo y no regulado del uso de la IA en el lugar de trabajo. Un estudio revela que más del 80 % de los empleados utilizan herramientas de IA no aprobadas por la empresa (UpGuard). Además, más de la mitad de los usuarios de IA generativa afirman utilizarla al menos ocasionalmente y sin declararlo; y casi el 50 % opera a través de cuentas personales, completamente fuera del control corporativo (Netskope). La seguridad de los datos es especialmente crítica: el 38 % de los trabajadores admite compartir datos confidenciales con plataformas de IA sin autorización, mientras que el 52 % de quienes utilizan estas herramientas nunca ha recibido formación específica sobre el tema (CybSafe & National Cybersecurity Alliance).

Como observó Max Weber, la racionalización administrativa no se produce mediante decisiones aisladas, sino a través de adaptaciones progresivas de las prácticas. La IA se inscribe en esta tendencia: no como una disrupción repentina, sino como un acelerador silencioso de los métodos operativos existentes.

El verdadero riesgo no reside en el uso de la IA en sí, sino en que dicho uso se produzca fuera de cualquier marco de rendición de cuentas institucional, en una zona gris que dificulta la rendición de cuentas de las decisiones, los errores y las consecuencias.

En muchos aspectos, la administración pública se caracteriza estructuralmente por procedimientos repetitivos, secuencias codificadas y actos estandarizados.

Precisamente por ello, la IA podría representar una oportunidad significativa, no para sustituir a los responsables de la toma de decisiones públicas, sino para liberar al personal de tareas mecánicas, permitiendo a los funcionarios centrarse en evaluaciones con un mayor contenido legal y discrecional.

Sin embargo, en ausencia de un marco regulatorio claro y de herramientas integradas institucionalmente en los sistemas de información pública, se produce un efecto paradójico. Los funcionarios individuales, que carecen de la capacidad técnica para integrar de forma independiente la IA con los sistemas de protocolo, gestión documental o flujos de trabajo procedimentales —normalmente regidos por plataformas centrales sujetas a rigurosas restricciones de seguridad, auditabilidad y trazabilidad—, acaban utilizando la inteligencia artificial principalmente en fases altamente cognitivas: redacción de disposiciones, justificaciones, notas de investigación y resúmenes de evaluación.

En otras palabras, precisamente las actividades que impactan más directamente en la esfera jurídica de los ciudadanos se están convirtiendo en las más expuestas a formas de delegación informal y no regulada, mientras que las actividades puramente ejecutivas y procedimentales permanecen rígidamente ligadas a los sistemas oficiales. Esto crea una especie de «asimetría de la automatización»:

las funciones menos sensibles siguen estando supervisadas por la organización, mientras que las más sensibles corren el riesgo de ser realizadas con herramientas individuales e imposibles de rastrear, sin protocolos de rendición de cuentas.

Este fenómeno ya se ha puesto de manifiesto a nivel internacional en documentos de la OCDE sobre la transformación digital del sector público y en las directrices interpretativas iniciales de la Ley Europea de IA, que enfatizan la necesidad de garantizar la rendición de cuentas, la supervisión humana efectiva y la trazabilidad de las decisiones asistidas por sistemas de IA, precisamente para evitar que el uso individual y no institucionalizado produzca decisiones «opacas» en términos de responsabilidad administrativa.

De ello se deduce que la cuestión no radica tanto en si los funcionarios utilizan inteligencia artificial —un fenómeno ya inevitable—, sino en si dicho uso se integra en las infraestructuras organizativas oficiales, dotadas de registros de uso, criterios de validación, políticas de control y responsabilidades claramente definidas. Sin esta integración, la administración corre el riesgo de encontrarse en la singular situación de que la IA pueda, de hecho, contribuir a la redacción de una disposición administrativa que podría afectar los derechos, los intereses legítimos o la situación económica de los ciudadanos, sin que la organización cuente con las herramientas necesarias para supervisar cómo se ha utilizado este apoyo, con qué datos y según qué criterios.

De ahí la necesidad cada vez más evidente de pasar del uso espontáneo e individual de la IA a una adopción institucional regulada, capaz de integrar la innovación tecnológica dentro de los principios tradicionales de la actuación administrativa —legalidad, transparencia, rendición de cuentas y control—, evitando al mismo tiempo que la aceleración tecnológica, paradójicamente, conlleve una disminución de las garantías.

Capítulo 2

SUPERAR LA CRISIS DE LA GOBERNANZA

(Guido Giusti)

El marco regulatorio como infraestructura de confianza

La regulación de la inteligencia artificial se produce hoy en un contexto de transformación institucional caracterizado por una asincronía significativa: la innovación tecnológica evoluciona exponencialmente, mientras que la adaptación de las estructuras administrativas sigue necesariamente el ritmo de la democracia y las garantías, vinculadas a la producción de normativas y la reorganización de competencias.

En esta fase de transición, las administraciones públicas operan dentro de un marco regulatorio cada vez más consolidado, en el que las herramientas avanzadas suelen adoptarse antes de integrarse plenamente en los modelos organizativos y los sistemas de control institucional.

Sin una gobernanza explícita, la tecnología tiende a propagarse por «inercia operativa», impulsada por la necesidad de agilizar los procesos y mejorar la eficiencia diaria, más que por una estrategia consciente. El verdadero riesgo no reside en la introducción de la tecnología, sino en su adopción silenciosa: el uso no regulado de herramientas que impactan directamente en el ejercicio de los derechos.

En este sentido, la intuición de Lawrence Lessig —el código es ley— cobra renovada relevancia: si no se regula, la arquitectura del software acaba produciendo efectos normativos de facto, dictando las modalidades concretas de ejercicio del poder administrativo.

El problema no solo afecta a los resultados (decisiones), sino también, y sobre todo, a los datos de entrada. El principio informático de «si introduces basura, obtienes basura» adquiere aquí relevancia jurídica: datos incompletos, obsoletos o con sesgo histórico pueden generar decisiones formalmente eficientes, pero esencialmente ilegítimas. Aún más crítico es el uso de plataformas externas para el procesamiento de datos públicos, lo que plantea un problema de soberanía de la información: la entidad pública debe correr el riesgo de perder el control sobre su base de conocimiento estratégico, debilitando su papel como garante de los datos.

El uso no regulado también fomenta fenómenos de irresponsabilidad en la toma de decisiones: el error se atribuye a la «máquina», mientras que la decisión parece técnicamente inevitable. Este es el fenómeno del «lavado matemático»: encubrir decisiones probabilísticas con objetividad matemática. Sin embargo, el sistema jurídico no reconoce la «responsabilidad algorítmica»: la responsabilidad siempre recae en el ser humano y la organización. La IA no es un oráculo de la verdad, sino una herramienta de cálculo que requiere interpretación, verificación y, cuando sea necesario, la valentía de expresar una disidencia razonada por parte del funcionario.

Para gestionar esta complejidad, el sistema jurídico actual ofrece una arquitectura regulatoria multinivel, estructurada en niveles complementarios.

La base de esta estructura jurídica es el Reglamento General de Protección de Datos (RGPD). Lejos de ser un mero instrumento burocrático, el Reglamento (UE) 2016/679 introdujo el principio fundamental de la rendición de cuentas en el sistema europeo, exigiendo a las administraciones no solo el cumplimiento de las normas, sino también la capacidad de demostrarlo mediante la documentación proactiva de las decisiones organizativas. El núcleo de esta protección reside en el artículo 22, que prohíbe someter a las personas a decisiones basadas únicamente en el tratamiento automatizado que produzcan efectos jurídicos o afecten significativamente a su esfera personal, exigiendo una supervisión humana efectiva, y no meramente formal.

El alcance de esta prohibición fue aclarado por el Tribunal de Justicia de la Unión Europea en su sentencia del 7 de diciembre de 2023, en el asunto C-634/21 (Schufa Holding AG). Los jueces europeos dictaminaron que la generación automatizada de un valor de probabilidad (como una puntuación de fiabilidad) constituye una «decisión basada únicamente en el tratamiento automatizado» en el sentido del artículo 22, apartado 1, del RGPD, si dicho valor determina de forma significativa la decisión final adoptada por un tercero. Este principio es crucial para la actuación administrativa: el resultado de un algoritmo no puede predeterminar efectivamente el resultado de un procedimiento. La prohibición europea impide que la intervención del órgano decisorio público se reduzca a una mera aprobación formal, evitando que el algoritmo se transforme de una herramienta de apoyo a las investigaciones en un instrumento decisorio encubierto.

Este primer nivel de protección de datos se complementa con el Reglamento Europeo sobre Inteligencia Artificial (Ley de IA). Mientras que el RGPD protege a las personas, el Reglamento (UE) 2024/1689 regula la herramienta, adop-

tando un enfoque basado en el riesgo. Una gran parte de las aplicaciones de la administración pública se clasifican como de "alto riesgo": desde sistemas para la prestación de servicios esenciales y prestaciones sociales hasta procedimientos de selección de personal, pasando por sistemas predictivos utilizados para evaluaciones de comportamiento o toma de decisiones.

En estos ámbitos, el legislador europeo impone requisitos operativos rigurosos, que incluyen evaluaciones de impacto en los derechos fundamentales, altos estándares de gobernanza de datos y requisitos de transparencia técnica (explicabilidad), para que el funcionamiento de los sistemas no resulte opaco para los afectados.

La Ley italiana de Inteligencia Artificial (Ley 132/2025), que traslada la legislación supranacional al ámbito nacional, actúa como enlace institucional. Esta legislación nacional evita duplicar las obligaciones sustantivas establecidas en la Ley de IA, centrándose en definir la gobernanza interna e identificar las autoridades competentes - incluidas la Agencia Nacional de Ciberseguridad (ACN) y la Agencia para la Italia Digital (AgID) -, así como los mecanismos de coordinación entre las administraciones. El objetivo es prevenir la fragmentación y garantizar que la transición digital se produzca de forma uniforme y segura en todo el país.

En este contexto, el artículo 14 de la ley, que aborda específicamente el uso de la inteligencia artificial en la administración pública, adquiere una importancia fundamental. La ley establece un marco operativo estricto: si bien la IA está autorizada para aumentar la eficiencia y «reducir el tiempo necesario para completar los trámites», el legislador establece inequívocamente que su uso debe ser exclusivamente «instrumental y de apoyo a la actividad humana». El artículo 14 establece la transparencia algorítmica como un deber institucional, exigiendo a las administraciones que garanticen siempre que las partes interesadas tengan "conocimiento de su funcionamiento y trazabilidad de su uso", reiterando que el poder y la responsabilidad de las decisiones finales nunca pueden delegarse en las máquinas.

El ciclo regulatorio se cierra a nivel estrictamente operativo mediante las Directrices AgID para la adopción, adquisición y desarrollo de sistemas de IA en la Administración Pública, previstas en el artículo 71 del Código de Administración Digital y el Plan Trienal de TI en la Administración Pública. El propio Código de Administración Digital se encuentra actualmente en un proceso de profunda actualización estructural, con el objetivo de adaptar su marco a los desafíos sin precedentes que plantea la innovación tecnológica. Como reflejo de esta transición institucional crucial, en febrero de 2026 se creó una Comisión especial, presidida por el profesor Aristide Police, para revisar el Código de Ad-

ministración Digital y regular los métodos digitales de producción regulatoria. Este esfuerzo de reforma confirma inequívocamente la necesidad de un ecosistema regulatorio dinámico capaz de adaptarse constantemente al progreso técnico.

El papel de las mencionadas Directrices AgID se enmarca dentro de este marco en rápida evolución. Estas directrices traducen las normas jurídicas en estándares técnicos y protocolos organizativos: si bien se clasifican formalmente como derecho blando, en la práctica administrativa adquieren una función sustancialmente vinculante, ya que definen los requisitos de cumplimiento necesarios para la adquisición y el funcionamiento de sistemas algorítmicos. Mediante estas normas, los principios de transparencia y rendición de cuentas se transforman en requisitos informáticos concretos para la auditabilidad, la trazabilidad y los registros operativos, lo que permite reconstruir a posteriori el proceso de toma de decisiones.

Esta infraestructura regulatoria integrada tiene un propósito específico: generar confianza institucional. Su objetivo es evitar que la innovación cree zonas grises en las que las autoridades públicas operen al margen de las garantías de los procedimientos administrativos. El uso no declarado de la IA representa no solo un riesgo tecnológico, sino también un indicador de inmadurez en la gobernanza: pone de manifiesto la lentitud con la que las organizaciones legales y administrativas son capaces de incorporar innovaciones que, en la práctica diaria de las oficinas, ya se han vuelto operativas.

Capítulo 3

EL PAPEL DE LA DEFENSA CIVIL

(Guido Giusti)

Nuevos horizontes en la protección de los derechos

En el contexto de la nueva arquitectura regulatoria para la inteligencia artificial que emerge a nivel europeo y nacional, las instituciones de garantía también se ven obligadas a redefinir su función.

En el panorama institucional actual, la misión del Defensor del Pueblo está experimentando una profunda transformación. Es importante recordar que el Defensor del Pueblo es, ante todo, un órgano de garantía autónomo e independiente, cuyo ámbito de actuación se extiende no solo a la administración pública, sino también —en muchas jurisdicciones, incluida la italiana— a entidades privadas que gestionan servicios públicos esenciales. Esta posición singular, a medio camino entre el ciudadano y el aparato administrativo, caracterizada por funciones de persuasión moral y resolución de conflictos no jurisdiccionales, no es una reliquia nostálgica de una era predigital. Por el contrario, la flexibilidad de esta función la convierte en una de las herramientas institucionales más idóneas para operar en la nueva frontera inmaterial de la protección.

La burocracia tradicional no desaparece, continúa existiendo en sus rituales, plazos y formas organizativas, sin embargo, junto a la dimensión material de las oficinas y los actos administrativos, se desarrolla una segunda dimensión, menos visible pero cada vez más decisiva, en la que el aparato público se configura a través de sistemas de información, plataformas digitales y procedimientos automatizados. Si bien los ciudadanos siguen interactuando con la administración en ventanillas, mediante formularios y disposiciones formales, las decisiones que les afectan se toman cada vez más dentro de procesos de información que operan "previamente" al acto final, organizando las prioridades, los plazos y los métodos de tramitación de las solicitudes.

La literatura ha representado a menudo la materialidad de la burocracia mediante la imagen de una secuencia interminable de sellos y certificaciones. Ennio Flaiano la describió como una especie de liturgia administrativa, compuesta por actos que se multiplican y se legitiman mutuamente, evocando esa "caída de sellos" que, más que garantizar la decisión, a veces parece sustituirla.

En procedimientos administrativos altamente serializados, como los servicios

de registro, la concesión de prestaciones sociales, la asignación de vivienda pública o la gestión de exenciones fiscales, los sistemas algorítmicos diseñados adecuadamente pueden aumentar eficazmente la capacidad de procesamiento de solicitudes, reducir los tiempos de respuesta y disminuir la acumulación de trámites. En estos contextos, la automatización puede contribuir a mejorar la eficiencia organizativa y garantizar una mayor uniformidad en la aplicación de los criterios normativos.

Sin embargo, la eficiencia no es el único parámetro que determina la legitimidad y la calidad de la actuación administrativa. La realidad inevitablemente presenta situaciones que no pueden atribuirse completamente a esquemas predeterminados: discrepancias entre bases de datos, condiciones subjetivas atípicas, errores materiales o circunstancias que requieren una interpretación de la ley. En estos casos, un sistema rígidamente paramétrico puede producir resultados formalmente coherentes, pero sustancialmente insuficientes dada la complejidad del caso específico.

Por este motivo, la introducción de la IA en los procedimientos administrativos exige claras garantías: transparencia en los criterios utilizados, posibilidad de una intervención humana efectiva, herramientas de corrección y canales de revisión accesibles. La tecnología puede respaldar las decisiones, pero no puede eximirlas de su responsabilidad.

En este contexto, el papel del Defensor del Pueblo, al igual que en la política, no debe ser ni entusiasta ni catastrófico. Simplemente debe asumir su función de garantía, verificando que el uso de herramientas algorítmicas no conlleve restricciones indebidas a los derechos, asegurando que la revisión humana sea posible de manera efectiva en casos no estandarizados y contribuyendo a mantener un equilibrio entre la eficiencia organizativa y la protección sustantiva de las personas.

Si la automatización permite a las oficinas agilizar la gestión de procedimientos rutinarios, esto puede traducirse en una mayor disponibilidad de recursos para casos complejos y situaciones que requieren atención y evaluación personalizadas. Desde esta perspectiva, la tecnología y la protección no son alternativas, sino que deben integrarse en un marco donde la rapidez operativa no prevalezca sobre la equidad del caso específico, ni la cautela paralice la innovación organizativa.

Esta transformación modifica el propósito mismo de la protección. Tradicionalmente, el control se ha centrado en el acto administrativo final, como expresión legal de las intenciones de la institución. Sin embargo, hoy en día, una parte

cada vez mayor del proceso se desarrolla mucho antes, en etapas preliminares automatizadas o controladas por software. Consideremos casos específicos: la gestión automatizada de listas de espera en el sector sanitario, la priorización del acceso a prestaciones sociales, la clasificación de solicitudes de acceso a documentos, la selección de casos a procesar o la organización de colas digitales en los servicios públicos. En estos contextos, es dentro del proceso informático donde se determinan los plazos, se acumulan las demoras y surgen los silencios administrativos. El acto final corre así el riesgo de quedar reducido a una mera «fachada legal» que ratifica una evaluación previamente realizada.

Si el Defensor del Pueblo se limitara a intervenir en etapas posteriores, solo llegaría cuando el daño ya se hubiera cristalizado. El verdadero desafío, sin embargo, reside en extender su alcance a los procedimientos informatizados, afirmando la accesibilidad, la comprensibilidad y la verificabilidad de la lógica que rige el software público.

La literatura y el imaginario colectivo han representado repetidamente la impotencia del ciudadano frente a los mecanismos administrativos: desde el laberinto del Castillo de Kafka hasta la famosa «Casa que enloquece a la gente», en la que Astérix y Obélix se ven obligados a perseguir un pase de la A38. La digitalización no elimina el riesgo de estos laberintos; más bien, puede hacerlos más silenciosos y menos visibles, transformando la complejidad procedimental en opacidad algorítmica.

Ante el riesgo de una toma de decisiones opaca, el Defensor del Pueblo también está llamado a asumir el papel de garante de la transparencia técnica. Cuando la administración justifica una exclusión o demora simplemente remitiéndose al resultado del sistema informático, el Defensor debe exigir la trazabilidad de la "contaminación tecnológica", verificando que el algoritmo no oculte sesgos discriminatorios derivados de datos históricos distorsionados y que sea posible reconstruir la ruta lógica de la decisión.

Esta necesidad de reconstrucción retrospectiva no es un mero capricho tecnológico, sino que impacta directamente en la esencia misma del Estado de derecho: la obligación de fundamentar las decisiones, establecida en el artículo 3 de la Ley n.º 241, de 7 de agosto de 1990. Juristas y la jurisprudencia administrativa más autorizada coinciden en que una medida basada en un algoritmo desconocido es radicalmente ilegítima, ya que carece del mínimo contenido esencial de razonamiento. El Consejo de Estado, con las sentencias fundamentales de la Sección VI (en particular, las sentencias n.º 2270 y n.º 8472 de 2019), ha aclarado inequívocamente que el software debe considerarse en todos los aspectos como un «acto administrativo informático» y que el algoritmo debe clasificarse legalmente como un «módulo procesal».

De esta definición precisa se desprende que la regla algorítmica, aun cuando se exprese en forma matemática, debe estar sujeta a los principios generales de la actividad administrativa: la justificación de la medida debe necesariamente traducirse en una explicación de la lógica informática adoptada (explicabilidad). Un acto que simplemente incorpora pasivamente un resultado generado por un sistema opaco impide reconstruir el proceso lógico-jurídico seguido por la institución, socavando así la función de garantizar la justificación e impidiendo cualquier derecho efectivo de defensa para el ciudadano.

Sin embargo, la clasificación del algoritmo como un acto administrativo teóricamente aparente plantea una cuestión crucial en el plano puramente operativo: ¿Posee el Defensor del Pueblo la pericia necesaria para evaluar y decidir sobre la revisión de una solicitud de acceso a documentos que se refieren, por ejemplo, al código fuente de un programa informático o a los archivos de registro de un sistema automatizado de toma de decisiones?

Ante una administración que niega el acceso a los ciudadanos alegando secreto industrial, derechos de autor o la impenetrabilidad de una arquitectura informática llave en mano adquirida a un proveedor privado, la pericia de un experto jurídico puro corre el riesgo de resultar insuficiente. Para garantizar que la respuesta a una solicitud de revisión no se reduzca al mero cumplimiento formal de las limitaciones técnicas de la institución, la Defensoría del Pueblo del futuro debe adoptar una colaboración interdisciplinaria rigurosa. Será esencial integrar conocimientos técnicos y de TI capaces de apoyar a la Defensoría en el delicado equilibrio entre el derecho público a la transparencia (explicabilidad) y las restricciones comerciales o de seguridad asociadas al código informático.

De este modo, la Defensoría del Pueblo contribuye a contrarrestar el riesgo de lagunas en la rendición de cuentas, reiterando que detrás de cada error —incluso cuando está mediado por sistemas automatizados y protegido por barreras técnicas— siempre existe una responsabilidad institucional, humana y organizativa plenamente revisable.

Pero la inteligencia artificial no es solo un objeto de monitoreo, también puede convertirse en una herramienta para la defensa activa de los derechos. Las oficinas del Defensor del Pueblo reciben diariamente un flujo masivo y heterogéneo de quejas —correos electrónicos, correos electrónicos certificados, llamadas telefónicas y solicitudes digitales—, a menudo redactadas bajo un intenso estrés emocional, donde se entrelazan hechos objetivos y percepciones subjetivas, lo que dificulta la identificación inmediata de cuestiones legalmente relevantes. En esta fase de "clasificación inicial", la IA puede actuar como una infraestructura de ordenación lógica. Las herramientas avanzadas de procesamiento del lenguaje natural pueden extraer automáticamente los elementos esenciales

de las quejas, identificando recurrencias léxicas que señalan categorías típicas de dificultades —retrasos crónicos, denegaciones de acceso, errores materiales o disfunciones sistémicas— y, por lo tanto, permiten identificar patrones recurrentes difíciles de detectar mediante el análisis manual de los expedientes.

Desde esta perspectiva, la inteligencia artificial apoya la transición de la protección episódica de casos individuales a la protección sistémica de los derechos, lo que permite al Defensor del Pueblo identificar rápidamente anomalías organizativas o disparidades regionales en el trato e intervenir antes de que se conviertan en litigios generalizados. Los ciudadanos no se reducen a un mero conjunto estadístico, sino que se convierten en el punto de partida para una acción institucional más informada, capaz de transformar la escucha individual en conocimiento sistémico.

En conclusión, la inteligencia artificial no sustituye el juicio humano, sino que lo potencia. Al liberar al Defensor del Pueblo de tareas repetitivas de clasificación y análisis preliminar, permite que los recursos se centren en aquello que ningún algoritmo puede replicar: la capacidad de escuchar, gestionar excepciones complejas, mediar entre la administración y la ciudadanía, y ejercer influencia moral institucional. El Defensor del Pueblo del futuro no será un técnico informático, sino un jurista «aumentado», capaz de cuestionar la tecnología para obligarla a cumplir con los principios de legalidad, justicia y buena administración.

Capítulo 4

DEFENSA CIVIL Y TRANSICIÓN DIGITAL

(Guido Giusti)

Propuestas y prácticas operativas.

Más allá de las premisas teóricas, es necesario examinar cómo los principios de transparencia y rendición de cuentas pueden traducirse en prácticas operativas concretas dentro de una oficina del defensor del pueblo moderna. En este sentido, las conversaciones con colegas de gran autoridad —desde Marino Fardelli, presidente de la Coordinación Nacional de Defensores del Pueblo, hasta Francesco Cozzi, defensor del pueblo de la región de Liguria— han puesto de manifiesto un amplio consenso en un aspecto fundamental, no existe la necesidad ni el deseo de automatizar la resolución de controversias. El objetivo de utilizar la inteligencia artificial es diferente y, solo aparentemente, menos ambicioso, evitar que el proceso de resolución de controversias se disperse en una miríada de microactividades de escaso valor añadido —registro, clasificación, catalogación— que consumen un tiempo valioso.

El objetivo es liberar recursos cognitivos para aquello que ninguna máquina puede replicar: la investigación sustantiva, la escucha empática a los ciudadanos y la mediación relacional compleja con la administración.

La fase de entrada: Del triaje al protocolo inteligente

Estos principios encuentran su primera aplicación en la gestión del flujo de correos electrónicos entrantes. La experiencia de grandes administraciones como el INPS —que gestiona millones de correos electrónicos certificados anualmente gracias a sistemas de clasificación automática— demuestra cómo la IA puede transformar un problema de volumen en una oportunidad de eficiencia. Aplicada a la Oficina del Defensor del Pueblo, esta tecnología transforma una narrativa subjetiva y a menudo desorganizada (el correo electrónico de un ciudadano) en datos estructurados. Un sistema de triaje inteligente puede leer la solicitud, identificar la administración competente, recomendar su asignación al funcionario especializado y, sobre todo, señalar cualquier asunto urgente. Las decisiones no se toman “en lugar” de la oficina, sino que preparan el terreno para una intervención humana oportuna.

El filtro de elegibilidad.

Una segunda aplicación crucial se refiere a la fase previa a la investigación. El Defensor del Pueblo debe verificar preliminarmente su competencia y la ausencia de impedimentos (por ejemplo, asuntos penales, disputas entre particulares). Durante esta fase, la IA puede actuar como filtro de apoyo, realizando comprobaciones formales que liberan a la oficina de tareas más mecánicas:

• Verificación de legitimidad: Análisis preliminar del interés jurídico para iniciar el procedimiento.

• Ámbito de competencia: Mapeo automático de entidades supervisadas, rechazando solicitudes dirigidas por administraciones estatales u órganos judiciales.

• Cálculo de plazos: Verificación computacional de la puntualidad (p. ej., revisión de 30 días para completar el plazo de acceso a documentos), detectando inmediatamente cualquier retraso. El sistema no solicita nada hasta que notifica al operador cualquier inconsistencia, generando un formulario de admisibilidad que el operador humano solo debe validar

La investigación: reconstrucción regulatoria y protección sistémica

En el centro del proceso —la investigación preliminar— la IA evoluciona de un filtro a un asistente de investigación. Los servicios del Defensor del Pueblo se basan en la reconstrucción de hechos y normativas. En este contexto, los algoritmos de búsqueda semántica pueden ayudar a reconstruir el marco normativo, destacando las disposiciones derogadas o las modificaciones recientes, y ordenando cronológicamente la documentación (creando un verdadero «expediente vivo»), lo que permite detectar discrepancias entre lo declarado y lo probado.

Pero el verdadero salto cualitativo reside en la protección sistémica. Cuando el software identifica decenas de expedientes con la misma anomalía (por ejemplo, una demora sistemática en una oficina específica o el rechazo reiterado de una solicitud), el Defensor del Pueblo ya no se enfrenta a un fallo aislado, sino a la aparición de una mala administración estructural.

La posibilidad de utilizar la inteligencia artificial como herramienta para evaluar la calidad de la acción pública no es, sin embargo, una mera sugerencia teórica. El proyecto SAVIA (Inteligencia Artificial para la Calidad de las Leyes), concebido por la Asamblea Legislativa de la Región Emilia-Romaña en colaboración con CINECA, ofrece una demostración concreta y pionera de este potencial. Mediante el uso de modelos lingüísticos avanzados (MLA), SAVIA consulta

bases de datos regionales para apoyar a los legisladores en la evaluación ex ante y ex post del impacto de las normativas, garantizando al mismo tiempo una mayor transparencia y participación ciudadana.

Al adoptar este mismo enfoque analítico y trasladarlo del ámbito legislativo al de la protección de derechos, la inteligencia artificial permite al Defensor del Pueblo dar un paso decisivo: pasar definitivamente del tratamiento de síntomas individuales al diagnóstico de patologías administrativas.

Esta capacidad de diagnóstico abre el camino a una de las aplicaciones más prometedoras de la inteligencia artificial generativa al servicio de las instituciones: la planificación de escenarios. La IA puede procesar rápidamente enormes cantidades de datos históricos y precedentes administrativos para crear "borradores de escenarios" predictivos. Esta evolución resulta crucial para el ejercicio de la función del Defensor del Pueblo: ya sea para predecir el impacto de un cambio repentino en los criterios de acceso a la vivienda pública o para anticipar la oleada de quejas derivada de la introducción de un nuevo y complejo sistema de precios locales, la IA generativa puede simular rápidamente el impacto en los ciudadanos basándose en eventos similares del pasado.

De este modo, el papel del Defensor del Pueblo da un paso más allá: la modelización predictiva nos permite ir más allá de la lógica de la intervención a posteriori, lo que posibilita que la Oficina alerte a la administración con antelación y sugiera medidas organizativas antes de que la criticidad procesal se convierta en una violación generalizada y flagrante de los derechos de los ciudadanos.

La fase de toma de decisiones

Llegamos finalmente al momento crucial y más delicado de todo el proceso: la redacción del documento final, ya sea una solicitud de cumplimiento, una recomendación o una resolución. En este punto, es fundamental actuar con la máxima cautela. Como aclara el Reglamento (UE) 2024/1689 (la denominada Ley de IA), los sistemas de inteligencia artificial destinados a respaldar decisiones administrativas o garantizar funciones generalmente se clasifican como de "Alto Riesgo". Sin embargo, el propio legislador europeo distingue pragmáticamente entre las "actividades auxiliares" —permitidas con menor rigor formal— y la "decisión propiamente dicha". La inteligencia artificial puede, sin duda, respaldar la redacción formal, mejorar la claridad del lenguaje o verificar la coherencia lógica con los precedentes de la Oficina, pero nunca podrá sustituir el criterio de equidad. El papel del Defensor del Pueblo, por su propia naturaleza, es la expresión de un delicado equilibrio institucional y una sensibilidad imparcial necesaria para evaluar los innumerables matices de cada caso específico, a menudo irreductibles a una lógica binaria rígida.

Incluso la jurisprudencia administrativa más autorizada ha delineado claramente este camino. El Consejo de Estado, con la conocida resolución de la Sección VI, n.º 2270, del 8 de abril de 2019, declaró que la automatización no debe ser demonizada, sino fomentada cuando permite reducir la negligencia o la intencionalidad humanas, con una condición esencial: que nunca se abandonen los principios fundamentales de transparencia y razonamiento. El algoritmo, en última instancia, no es un oráculo misterioso e incuestionable, sino una simple «regla técnica» que debe permanecer siempre inteligible y abierta a la revisión.

En los años posteriores, los principios establecidos por la Asamblea Plenaria en relación con los algoritmos han sido frecuentemente objeto de controversias, disputadas entre los defensores de la automatización total y los detractores a priori del medio tecnológico. Sin embargo, con la amplia difusión de sistemas basados en modelos lingüísticos a gran escala (MLE), hemos sido testigos de una maduración progresiva del debate y de una jurisprudencia más equilibrada, capaz de situarse "en el medio" entre estos dos extremos.

La reciente directriz del Tribunal Administrativo Regional del Lacio (TAR) (expresada más recientemente en la sentencia n.º 1895/2026) se enmarca en este contexto en constante evolución. Dicha directriz aclara que la automatización de los procedimientos nunca puede conllevar la exclusión indiscriminada de datos útiles ni la omisión del análisis crítico de los resultados de las máquinas. En las decisiones administrativas digitalizadas, lo que se denomina una «reserva de humanidad» —una supervisión humana eficaz y exhaustiva— sigue siendo esencial.

La Administración, en todas sus ramas, debe mantener un control efectivo y la plena capacidad de intervención en las decisiones generadas por sistemas automatizados. Este imperativo se fundamenta en los pilares constitucionales de nuestro ordenamiento jurídico (artículos 3, 24 y 97 de la Constitución), así como en las sólidas garantías de la Ley 241/1990 y el Código de Administración Digital. En este contexto, la Ley de IA desempeña un papel crucial: si bien no siempre es directamente aplicable a los microprocedimientos internos individuales, sirve como un potente «parámetro interpretativo evolutivo». Su fundamento refuerza la obligación de transparencia y la plena revisabilidad de las decisiones algorítmicas, especialmente cuando se utilizan sistemas de alto riesgo, como ocurre en los procesos de selección pública. En consecuencia, incluso el estricto principio de la responsabilidad ciudadana se ve debilitado cuando se cumple el requisito sustantivo y el error se debe únicamente a la inflexibilidad del software.

La inteligencia artificial se incorpora a la Defensoría del Pueblo no como un juez algorítmico, sino como una herramienta para gestionar la complejidad. De

hecho, la tecnología puede liberar a la institución de cargas burocráticas y formales, permitiendo que el Defensor del Pueblo se mantenga fiel a su misión original: garantizar, con reflexión e independencia, que incluso en un mundo profundamente digitalizado, la Administración Pública conserve siempre un rostro humano.

Capítulo 5

OBSERVACIONES FINALES

(Guido Giusti)

Como hemos visto en las páginas anteriores, la inteligencia artificial ya se ha integrado en la vida cotidiana de las administraciones públicas mediante multitud de usos individuales, generalizados y, a menudo, invisibles.

Esta dinámica hace que sea inviable abordar el fenómeno únicamente mediante medidas prohibitivas. Cuando la administración simplemente prohíbe el uso de la inteligencia artificial sin ofrecer herramientas institucionales alternativas, el efecto no es la eliminación de la tecnología, sino su migración a formas de uso informales. Los empleados siguen utilizándola a través de dispositivos personales o cuentas privadas, introduciendo a veces información sensible en plataformas externas sobre las que la institución no tiene control. Paradójicamente, el intento de proteger a la organización del riesgo tecnológico acaba debilitando las mismas garantías de seguridad y trazabilidad que pretendía preservar.

La cuestión, por lo tanto, no es si se debe utilizar la inteligencia artificial, sino cómo integrarla en un marco institucional regulado. La verdadera elección no reside entre uso y prohibición, sino entre un uso espontáneo, individual y opaco, y un uso institucional, disciplinado y responsable.

En este contexto, la cuestión de las competencias adquiere una relevancia que trasciende la dimensión puramente técnica. La progresiva digitalización de los procedimientos administrativos implica que una parte cada vez mayor de las decisiones públicas se toman dentro de infraestructuras de información y sistemas de procesamiento de datos. Comprender el funcionamiento de estos sistemas no significa convertir a los abogados en ingenieros informáticos, sino evitar que las decisiones jurídicas se vean influenciadas progresivamente por herramientas tecnológicas que siguen siendo opacas para sus usuarios.

Para las instituciones de garantía, y en particular para el defensor del pueblo, esta transformación adquiere una relevancia aún mayor. El defensor del pueblo se creó históricamente para contrarrestar la rigidez y la opacidad de la burocracia tradicional, ofreciendo a los ciudadanos un foro de diálogo capaz de encauzar la actuación administrativa dentro de los parámetros de equidad y razonabilidad.

Hoy en día, sin embargo, una parte cada vez mayor de las decisiones admini-

strativas ya no se forma exclusivamente en el acto final, sino que se materializa en procedimientos digitales, sistemas de información y lógicas algorítmicas que operan antes de la disposición formal. En este contexto, el riesgo no reside únicamente en el error administrativo, sino también en la creciente incomprensibilidad de los procesos de toma de decisiones.

La función de garantía del defensor del pueblo está, por tanto, destinada a abordar cada vez más esta dimensión invisible de la actuación administrativa. No se trata de sustituir a las administraciones en la gestión tecnológica de los sistemas, sino de asegurar que los principios fundamentales del Estado de derecho sigan vigentes incluso en el entorno digital: la comprensibilidad de las decisiones, la rendición de cuentas de las instituciones y la posibilidad de impugnación ciudadana.

Desde esta perspectiva, además de ser una herramienta de regulación o control, la inteligencia artificial también puede convertirse en un apoyo para las actividades de garantía, permitiendo el análisis de grandes flujos de informes, la identificación de anomalías recurrentes y la transformación de la experiencia de casos individuales en conocimiento sistémico de las disfunciones administrativas.

Sin embargo, la cuestión fundamental sigue siendo institucional. La inteligencia artificial no sustituye la rendición de cuentas pública; al contrario, la hace aún más necesaria. Cuanto más dependan los procesos administrativos de sistemas complejos de procesamiento de datos, más esencial será preservar espacios para la comprensión, el control y la rendición de cuentas.

Por lo tanto, el reto para las administraciones y las instituciones reguladoras no reside en si utilizar o no la inteligencia artificial, sino en definir las condiciones bajo las cuales puede integrarse sin alterar el equilibrio entre la eficiencia administrativa y la protección de los derechos.

En este sentido, la cuestión de la inteligencia artificial en la administración pública no se limita a la innovación tecnológica, sino que implica la capacidad de las instituciones para adaptarse a un entorno de toma de decisiones cada vez más complejo sin perder de vista los principios que sustentan la legitimidad de la actuación administrativa.

SEGUNDA PARTE

NUEVAS TECNOLOGÍAS Y NUEVAS FRONTERAS DE PROTECCIÓN

Capítulo 1

LA INTELIGENCIA ARTIFICIAL EN FAVOR DE LA DEFENSA CIVIL Y LOS DERECHOS HUMANOS

(Ignacio Domínguez)

La defensa y protección de los derechos humanos están experimentando una profunda transformación en la actualidad. El contexto global —marcado por la acelerada digitalización, una crisis de confianza en las instituciones, conflictos complejos y nuevas formas de violación de derechos— exige que las instituciones de defensoría del pueblo evolucionen con igual rapidez y responsabilidad. En este escenario, las nuevas tecnologías ya no son un recurso opcional, sino herramientas estratégicas al servicio de la dignidad humana, la democracia y el Estado de derecho.

Comencemos con una idea simple:

Los derechos humanos no son un archivo. No son una práctica administrativa. No son un informe anual. Son personas reales, en tiempo real, que se enfrentan a quienes detentan el poder.

Durante décadas, los defensores del pueblo del mundo han sido la conciencia del Estado. Han observado, escuchado, documentado. Han defendido. Y esto ha sido esencial. Pero hoy, ya no es suficiente. El mundo ha cambiado.

Vivimos en una era donde las decisiones se toman en milisegundos, donde los datos crecen exponencialmente y donde la tecnología puede amplificar tanto la justicia como la injusticia. En este nuevo panorama, la pregunta no es si las instituciones de derechos humanos deben usar la tecnología. La verdadera pregunta es: ¿Qué tipo de futuro queremos construir?

La inteligencia artificial no es magia. Es una herramienta. Pero, si se usa correctamente, es una herramienta extraordinaria.

Puede ayudarnos a detectar patrones donde antes solo veíamos caos.

Puede ayudarnos a anticipar violaciones antes de que destruyan vidas.

Puede ayudarnos a poner a la víctima en el centro, no el expediente.

La IA no sustituye el juicio humano, lo libera. Aligera la carga de las tareas repe-

titivas para que podamos centrarnos en lo que realmente importa: las personas.

La ciberseguridad tampoco es simplemente una cuestión técnica: es una cuestión de confianza. Cuando una persona presta declaración ante un defensor del pueblo, entrega algo más que datos: entrega temor, esperanza y verdad. Si no protegemos esta información, incumplimos nuestro deber más básico. Sin seguridad digital, no hay privacidad, y sin privacidad, no hay derechos humanos.

Y luego está la computación cuántica.

Muchos dirán: «Aún no es relevante». Eso es lo que siempre se dice antes de que el mundo cambie.

La computación cuántica redefinirá la seguridad, la privacidad y la protección de la información. Prepararse hoy no es una exageración: es una responsabilidad. Los derechos humanos no pueden permitirse el lujo de quedarse atrás.

La computación cuántica ya es una realidad: opera comercialmente en algunas zonas de Asia desde antes de 2020 y ha sido utilizada y probada durante años por organizaciones como la NASA y grandes instituciones financieras multinacionales. También se esperan avances concretos en América Latina a partir de 2025.

Pero seamos claros, la tecnología por sí sola no salva a nadie. Sin valores, sin ética, sin supervisión humana, puede volverse fría, opaca y peligrosa; por lo tanto, el verdadero desafío para los defensores del pueblo del mundo no es tecnológico: es un desafío de liderazgo. Utilicemos la tecnología de acuerdo con principios. Diseñemos sistemas que respeten la dignidad humana. Decidamos que los algoritmos nunca deben ser superiores a las personas.

Las áreas de oportunidad son evidentes y esperan ser aprovechadas:

a) Pasar de la reacción a la prevención;

b) De la intuición a la evidencia;

c) De instituciones lentas a instituciones ágiles y humanas;

d) De relaciones que miran al pasado a decisiones que construyen el futuro.

Los beneficios son igualmente claros: mayor impacto, mayor credibilidad, mayor confianza, mayor justicia sustantiva.

Los defensores del pueblo no están llamados a defender procesos, sino personas.

La tecnología, si se usa bien, no deshumaniza, hace exactamente lo contrario. Devuelve el tiempo, la claridad y la concentración para ser más humanos. El futuro de los derechos humanos no solo estará escrito en leyes, se diseñará. Y quienes lo entienden hoy —quienes tienen el valor de unir ética, tecnología y visión— no solo protegerán los derechos, sino que ayudarán a transformar la forma en que el poder responde a la dignidad humana.

Este es el desafío. Esta es la oportunidad. Y, como siempre, el futuro pertenece a quienes tienen el valor de pensar diferente.

Capítulo 2

LA DEFENSA DE LOS DERECHOS Y EL DESAFÍO DE LA CIUDADANÍA DIGITAL

(Marino Fardelli)

El nuevo papel del Defensor del pueblo

Las transformaciones tecnológicas son una realidad cotidiana que impacta cada vez más la relación entre la ciudadanía y las administraciones públicas. En este contexto, el papel del Defensor del Pueblo se ve llamado a afrontar nuevos retos, pero también oportunidades sin precedentes, que están redefiniendo progresivamente su alcance y sus métodos de intervención.

La innovación, de hecho, no puede considerarse neutral. Impacta en los procedimientos, modifica el lenguaje, agiliza la toma de decisiones y, sobre todo, transforma la forma en que se ejercen y protegen los derechos fundamentales. Por ello, el Defensor del Pueblo no puede limitarse a observar el cambio: está llamado a ser un intérprete informado y un garante crítico, asegurando que el progreso tecnológico siga estando siempre enfocado en el servicio a la persona.

En este contexto, la inteligencia artificial se está incorporando gradualmente a los procesos de toma de decisiones de la administración pública, interviniendo en la gestión de los flujos de información, la selección de casos, el apoyo a la toma de decisiones y la automatización de las respuestas a la ciudadanía. Si bien estas herramientas pueden contribuir a mejorar la eficiencia, la rapidez y la coherencia de la actuación administrativa, también plantean importantes interrogantes en cuanto a la transparencia, la explicabilidad de las decisiones y la atribución de responsabilidades. El riesgo, no meramente teórico, reside en que el algoritmo se convierta en una pantalla tras la cual la administración eluda el control, haciendo opaco lo que debería permanecer accesible y verificable.

Desde esta perspectiva, el papel del Defensor del Pueblo adquiere una importancia estratégica. Su función es garantizar que las decisiones automatizadas sean comprensibles y estén debidamente justificadas, asegurar que el uso de la inteligencia artificial no produzca efectos discriminatorios —ni siquiera indirectos o involuntarios— y garantizar que la intervención humana correctiva siga siendo posible en todo momento, especialmente en los casos en que estén en juego los derechos fundamentales. La inteligencia artificial, desde esta perspectiva, no debe sustituir el juicio humano, sino complementarlo y apoyarlo,

contribuyendo a fortalecer su calidad y equidad.

Junto con la IA, la computación cuántica representa uno de los avances tecnológicos más significativos de nuestro tiempo. Si bien muchas de sus aplicaciones aún están en desarrollo, su impacto potencial en los sistemas públicos, la criptografía, la gestión de datos y la seguridad de la información ya se presenta considerable. Para el Defensor del Pueblo, la cuestión no se limita a la dimensión técnica, sino que adquiere una clara relevancia institucional y prospectiva. Ignorar la computación cuántica hoy significaría exponernos, en un futuro próximo, a nuevas vulnerabilidades en los sistemas de información pública, mayores riesgos para la protección de datos personales y posibles desequilibrios de poder entre quienes poseen estas tecnologías y quienes sufren sus efectos.

Esto subraya la necesidad de un enfoque preventivo, orientado a la rendición de cuentas pública en materia de innovación. En este sentido, el Defensor del Pueblo está llamado a promover la reflexión ética y jurídica antes de la implementación definitiva de estas tecnologías, evitando que decisiones de gran impacto se vuelvan irreversibles antes de que se comprendan y regulen plenamente.

La ciberseguridad, por su parte, dejó de ser hace tiempo un asunto confinado a los ámbitos técnico o militar para convertirse en un componente esencial de la protección de los derechos. Un sistema público vulnerable expone a los ciudadanos a riesgos concretos e inmediatos: pérdida de datos, violaciones de la privacidad, interrupciones en servicios esenciales y manipulación de la información. En este sentido, la ciberseguridad debe considerarse un requisito indispensable para la efectividad de los derechos, estrechamente vinculado al principio de buena gobernanza.

En este marco, el Defensor del Pueblo está llamado a desempeñar un papel activo, instando a la adopción de altos estándares de protección de datos, informando sobre problemas sistémicos que podrían socavar la confianza ciudadana y promoviendo una cultura de seguridad digital como elemento integral de la legalidad administrativa. Desde esta perspectiva, la ciberseguridad no se trata solo de proteger la infraestructura, sino también de salvaguardar la relación de confianza entre las instituciones y los ciudadanos, que es la base misma de la acción pública.

En un entorno cada vez más complejo y digitalizado, el papel del Defensor del Pueblo se enriquece con una dimensión adicional, adquiriendo las características de una mediación avanzada. Ya no se trata simplemente de intervenir en la relación entre la ciudadanía y la administración, sino también de velar por el delicado equilibrio entre la innovación tecnológica y los derechos humanos. Esto

exige competencias multidisciplinares, la capacidad de colaborar con expertos técnicos sin perder de vista la centralidad del individuo y una visión ética de la innovación, orientada hacia la inclusión, la transparencia y la rendición de cuentas.

Las nuevas tecnologías, si se gestionan adecuadamente, no deberían alejar a las instituciones de la ciudadanía, sino que pueden ser herramientas valiosas para acercarlas. Es precisamente en este ámbito donde el Defensor del Pueblo puede desempeñar un papel decisivo, erigiéndose como garante de un progreso inclusivo, no excluyente.

La inteligencia artificial, la computación cuántica y la ciberseguridad ya no son campos reservados a especialistas, sino cuestiones que impactan directamente en el funcionamiento de la democracia contemporánea. En este contexto, el papel del Defensor del Pueblo, por su propia naturaleza independiente y centrado en la protección de los derechos, se presenta como uno de los centros institucionales más idóneos para acompañar y orientar el cambio.

Gestionar la innovación, en definitiva, implica tomar decisiones informadas: priorizar la transparencia sobre la opacidad, la equidad sobre la automatización ciega, la seguridad sobre la improvisación. En este proceso, el Defensor del Pueblo puede - y debe - ser una guía fiable, capaz de orientar la acción pública con respeto a la dignidad humana.

Recomendaciones a la administración pública

La tecnología, si no va acompañada de una visión clara y una cultura administrativa orientada al servicio, corre el riesgo de convertirse en un factor de rigidez en lugar de simplificación. La digitalización de procedimientos ineficaces suele acelerar las disfunciones existentes, dificultando su corrección y haciéndolas menos comprensibles para la ciudadanía.

Cuando el Defensor del Pueblo interviene con recomendaciones, el enfoque no debe centrarse en la herramienta tecnológica en sí, sino en su uso por parte de la administración y sus efectos concretos en el ejercicio de los derechos. Las nuevas tecnologías pueden ofrecer un apoyo significativo a la actuación administrativa: mejoran la trazabilidad de los procedimientos, permiten una gestión de la información más ordenada, reducen los tiempos de respuesta y fomentan una mayor transparencia en las decisiones. En este sentido, también representan un valioso aliado para la labor del Defensor del Pueblo, quien puede basar sus evaluaciones en datos más claros, reconstrucciones más precisas y responsabilidades mejor identificadas.

Sin embargo, junto a estas innegables fortalezas, surgen debilidades estructurales que no son atribuibles a la tecnología, sino al contexto organizativo en el que se implementa. En muchas oficinas de la administración pública, la innovación digital coexiste con prácticas administrativas obsoletas, lo que genera duplicación de pasos, mayor carga de trabajo y confusión de roles y responsabilidades. Plataformas informáticas que no se comunican entre sí, sistemas explotados mínimamente y procedimientos digitales acompañados de archivos en papel son claros indicios de una transformación incompleta, a menudo llevada a cabo en lugar de gestionada.

Uno de los elementos más críticos que se desprenden de la experiencia del Defensor del Pueblo son los focos de resistencia interna presentes en muchas oficinas de la administración pública. Esta resistencia rara vez es explícita, pero está profundamente arraigada y se manifiesta a través de la inercia, la interpretación rígida y el uso defensivo de las normas y los procedimientos. En este contexto, la tecnología puede convertirse en un verdadero lastre: en lugar de fomentar el cambio, se utiliza como justificación para no tomar decisiones, para posponerlas o para negar a los ciudadanos soluciones razonables.

No es raro que las administraciones culpen al sistema informático de las demoras o denegaciones, como si el algoritmo o la plataforma fueran entidades autónomas e indiscutibles. Expresiones como «el sistema no lo permite» o «el procedimiento no ofrece alternativas» se convierten en fórmulas para eludir responsabilidades, ocultando a menudo una renuncia a la discreción y al sentido común. En estos casos, la tecnología no solo no mejora la relación con los ciudadanos, sino que contribuye a que esta se vuelva más distante y conflictiva.

Un claro ejemplo se refiere a la gestión de solicitudes digitales que presentan errores formales menores o fácilmente subsanables. En algunas oficinas, la imposibilidad de intervenir en el sistema informático se utiliza como motivo para rechazar la solicitud, sin considerar el fondo de la petición y sin ofrecer al ciudadano apoyo concreto para corregir el error. En tales circunstancias, la tecnología se convierte en un obstáculo y el principio de buenas prácticas administrativas se ve seriamente comprometido.

En estos contextos, las recomendaciones del Defensor del Pueblo adquieren un valor que trasciende la resolución de casos individuales. Pueden y deben destacar la necesidad de ir más allá de un enfoque meramente formal de la innovación, fomentando el uso de la tecnología en consonancia con el propósito público de la actuación administrativa. Formular recomendaciones también implica exigir responsabilidades a la administración, recordando que ningún sistema informático puede sustituir por completo el juicio humano y que la tecnología debe seguir siendo una herramienta al servicio de las personas, y no al revés.

Por lo tanto, la cuestión clave sigue siendo cultural. Sin un cambio profundo en nuestra concepción del trabajo público, toda innovación corre el riesgo de ser absorbida y neutralizada por las mismas dinámicas que pretendía superar. Las nuevas tecnologías solo pueden fortalecer la eficiencia, la transparencia y la equidad si se integran en un contexto que valore la responsabilidad individual, la formación continua y un enfoque orientado al servicio.

En este escenario, el Defensor del Pueblo puede desempeñar un papel decisivo como figura equilibradora y motivadora, capaz de identificar problemas sistémicos críticos y utilizar las recomendaciones como palanca para un cambio real. Superar la resistencia interna implica recuperar la capacidad de la Administración Pública para actuar con mayor agilidad, responder con mayor eficacia a las necesidades de la ciudadanía y utilizar las tecnologías para lo que realmente son: herramientas para mejorar la calidad de la democracia administrativa.

Capítulo 3

USO DE LAS NUEVAS TECNOLOGÍAS EN LA PROMOCIÓN Y EDUCACIÓN DE LOS DERECHOS HUMANOS EN EL CONTEXTO MEXICANO

(Ignacio Domínguez)

En el contexto internacional actual, la promoción y la educación en derechos humanos ya no pueden depender únicamente de los métodos tradicionales. La transformación digital ha redefinido la forma en que las sociedades aprenden, se informan y participan. Hoy en día, la inteligencia artificial, las plataformas digitales, el análisis de datos y el marketing digital estratégico se han convertido en herramientas clave para ampliar el alcance, la accesibilidad y el impacto de los programas de educación en derechos humanos a nivel mundial.

Desde una perspectiva de futuro - especialmente relevante para líderes académicos, consultores y responsables de políticas públicas - las nuevas tecnologías no reemplazan el enfoque humanista: lo enriquecen, lo optimizan y lo hacen cuantificable.

1. La inteligencia artificial como motor de la educación personalizada en derechos humanos.

La inteligencia artificial ha posibilitado el diseño de modelos educativos adaptativos, capaces de analizar el comportamiento del usuario y adaptar el contenido a su nivel de comprensión, idioma, contexto cultural y necesidades específicas.

A nivel internacional, organizaciones multilaterales y universidades han implementado plataformas de capacitación basadas en IA para preparar a funcionarios públicos en materia de derechos fundamentales, prevención de la discriminación y acceso a la justicia. Estos sistemas utilizan análisis de aprendizaje para identificar deficiencias en la capacitación y recomendar itinerarios educativos personalizados, lo que aumenta la eficacia pedagógica.

Por ejemplo, se han utilizado simuladores basados en IA para capacitar a fuerzas de seguridad y profesionales del derecho, recreando escenarios relacionados con el uso legítimo de la fuerza, el debido proceso y la protección de los derechos humanos, fortaleciendo así la toma de decisiones basada en un enfoque ético y normativo.

2. Marketing digital con enfoque social: visibilidad y concienciación estratégica.

El marketing digital se ha consolidado como una herramienta de gran impacto para la promoción de los derechos humanos. Mediante campañas segmentadas, contenido audiovisual, narración social y estrategias de posicionamiento digital, las instituciones pueden sensibilizar a grupos poblacionales específicos con mensajes claros y emocionalmente relevantes.

Las campañas digitales sobre igualdad, inclusión, derechos de la infancia y no discriminación han llegado a millones de personas a través de las redes sociales, demostrando que la educación en derechos humanos, cuando se comunica mediante técnicas de marketing digital, genera mayor comprensión, participación ciudadana y conciencia colectiva.

3. Plataformas digitales y educación abierta: acceso sin fronteras

Las aulas virtuales, los cursos en línea y los seminarios web especializados han revolucionado la educación en derechos humanos, eliminando las barreras geográficas y económicas.

Actualmente, miles de funcionarios públicos, académicos, estudiantes y defensores de derechos humanos acceden a contenido certificado sobre tratados internacionales, jurisprudencia en derechos humanos y gobernanza democrática a través de plataformas digitales equipadas con evaluaciones automatizadas y seguimiento formativo.

4. Big Data y análisis predictivo para políticas de educación en derechos humanos

El análisis de datos nos permite identificar patrones de violaciones de derechos y diseñar estrategias educativas específicas. Los paneles de control inteligentes permiten a las instituciones visualizar indicadores relacionados con la violencia, la discriminación, la exclusión social y el acceso a la justicia, facilitando así la toma de decisiones basadas en evidencia.

En contextos de crisis social, el monitoreo digital de las tendencias informativas se ha utilizado para detectar discursos de odio y diseñar campañas educativas preventivas orientadas a una cultura de paz y legalidad.

5. Tecnologías inmersivas y educación experiencial.

La realidad virtual y las tecnologías inmersivas han introducido un enfoque pedagógico innovador: aprender sobre derechos humanos a través de la experien-

cia.

Las simulaciones digitales nos permiten comprender situaciones de desplazamiento, discriminación o violaciones de derechos desde una perspectiva empática, fortaleciendo la conciencia institucional y social.

6. Ejemplo real en el contexto de los derechos humanos en México

En México, un ejemplo notable es la digitalización de programas educativos y campañas de promoción de derechos humanos impulsadas por instituciones como comisiones de derechos humanos y organizaciones académicas, que han integrado plataformas virtuales, redes sociales y herramientas digitales para la educación ciudadana.

Por ejemplo, en los últimos años, diversas instituciones públicas han implementado cursos masivos en línea sobre derechos humanos, género y derechos de grupos vulnerables, dirigidos a funcionarios públicos, estudiantes y público en general. Estos programas digitales han ampliado significativamente el alcance educativo, pasando de la capacitación presencial, necesariamente limitada, a cursos capaces de involucrar simultáneamente a miles de participantes en todo el país.

Asimismo, el uso de redes sociales y campañas digitales institucionales ha sido crucial para promover una cultura de derechos humanos en temas como la prevención de la violencia, los derechos de la infancia, los derechos de las mujeres y el acceso a la justicia. Mediante infografías, resúmenes educativos, seminarios web y contenido interactivo, se ha generado conciencia entre los jóvenes, un segmento altamente digitalizado.

Un ejemplo particularmente estratégico es el uso de plataformas tecnológicas para recibir denuncias en línea y para obtener orientación digital sobre cuestiones de derechos humanos, lo que reduce las barreras de acceso a la justicia, especialmente para las poblaciones vulnerables que viven en zonas rurales o con movilidad reducida. Esta transformación digital refuerza el principio de accesibilidad, pilar fundamental del sistema internacional de derechos humanos.

7. Riesgos éticos y gobernanza tecnológica en materia de derechos humanos

La integración tecnológica debe estar alineada con los principios de ética digital, protección de datos personales, transparencia algorítmica y no discriminación. En contextos como México y América Latina, donde la brecha digital sigue siendo un factor crítico, la implementación de tecnologías en el marco de los derechos humanos debe ser inclusiva, intercultural y contar con una sólida base

regulatoria.

Las instituciones deben garantizar que la inteligencia artificial y los sistemas digitales respeten la dignidad humana, eviten el sesgo algorítmico y cumplan con los estándares internacionales sobre derechos humanos y gobernanza tecnológica.

Conclusión estratégica y motivacional

La promoción y la educación en derechos humanos están entrando en una nueva era: digital, inteligente y estratégica. En países como México, donde los desafíos sociales coexisten con una creciente transformación tecnológica, el uso de la inteligencia artificial, las plataformas educativas digitales y el marketing social representan una oportunidad histórica para fortalecer la cultura de la legalidad y el respeto por los derechos fundamentales.

La tecnología, cuando se implementa con una visión ética, un enfoque pedagógico y un liderazgo institucional, no solo educa: empodera, previene violaciones y construye sociedades más conscientes, inclusivas y resilientes. En el siglo XXI, la defensa de los derechos humanos también se desarrolla en el entorno digital, y quienes dominen estas herramientas liderarán la transformación educativa y social del futuro.

Capítulo 4

PROTECCIÓN DE GRUPOS VULNERABLES

(Ignacio Domínguez)

Enfoque estratégico con aplicaciones de inteligencia artificial y su impacto positivo.

La protección de los grupos vulnerables es un pilar fundamental del sistema internacional de derechos humanos. En el contexto mexicano, caracterizado por la coexistencia de complejos desafíos sociales —como la desigualdad estructural, la brecha digital, la violencia de género, la migración y la exclusión económica—, el uso de la inteligencia artificial (IA) representa una herramienta potencialmente transformadora para fortalecer la prevención, la asistencia, la educación y la protección efectiva de los derechos humanos.

Desde una perspectiva contemporánea y de futuro, la IA no reemplaza la intervención institucional ni el enfoque humanista, sino que los potencia, haciéndolos más efectivos mediante el análisis predictivo, la automatización responsable, la accesibilidad digital y la toma de decisiones basada en datos y evidencia.

1. Protección de niños y adolescentes en entornos digitales

Los niños y niñas se encuentran entre los grupos más expuestos a riesgos como la ciberviolencia, la explotación, el abandono escolar y el ciberacoso. En este contexto, la inteligencia artificial (IA) nos permite monitorear situaciones de riesgo, prevenir violaciones y diseñar intervenciones educativas personalizadas basadas en un enfoque de derechos humanos.

Ejemplo de aplicación en México (IA y derechos de la infancia):

En el sistema educativo mexicano, las plataformas digitales basadas en IA pueden analizar indicadores como el ausentismo escolar, el rendimiento académico y el comportamiento en línea para identificar situaciones de riesgo, como el abandono escolar o la violencia doméstica, en una etapa temprana.

Por ejemplo, un sistema de análisis predictivo implementado en las escuelas públicas podría detectar cambios significativos en el rendimiento y la asistencia de un niño, lo que activaría automáticamente la intervención de los orientadores escolares y los trabajadores sociales, según un enfoque de protección integral.

Impacto positivo:

• Prevención temprana de violaciones de los derechos de la infancia;

• Reducción del abandono escolar;

• Intervenciones específicas para niños en situación de riesgo;

• Fortalecimiento del derecho a la educación y al desarrollo integral.

2. Protección de las mujeres y prevención de la violencia de género

La violencia contra las mujeres es un problema estructural en el contexto mexicano. La inteligencia artificial ofrece herramientas útiles para analizar patrones de violencia, mejorar los mecanismos de denuncia y fortalecer las políticas públicas de prevención.

Ejemplo de aplicación en México (IA y protección de las mujeres):

El uso de sistemas de IA en plataformas digitales de denuncia permite analizar el idioma, la frecuencia de las denuncias y la ubicación geográfica para identificar zonas de alto riesgo de violencia de género.

Por ejemplo, una aplicación institucional puede clasificar automáticamente las denuncias relacionadas con violencia doméstica, riesgo de feminicidio o acoso, priorizando los casos más urgentes y facilitando la intervención oportuna de las autoridades y las organizaciones de derechos humanos.

Impacto positivo:

• Mayor rapidez y eficacia en la respuesta institucional;

• Priorización de los casos más graves;

• Reducción de la victimización secundaria;

• Fortalecimiento del acceso a la justicia desde una perspectiva de género.

3. Protección de migrantes y refugiados

México, como país de tránsito y destino de migrantes, enfrenta importantes desafíos para proteger los derechos de los migrantes, quienes a menudo están expuestos a la discriminación, la violencia y la exclusión social.

Ejemplo de aplicación en México (IA y derechos de los migrantes):

Los sistemas de inteligencia artificial pueden integrarse en plataformas digitales multilingües, proporcionando información automatizada sobre derechos, servicios legales, atención médica y procedimientos de protección.

Un asistente virtual accesible desde dispositivos móviles puede ofrecer asistencia en tiempo real en varios idiomas —incluidos español, inglés e idiomas indígenas— informando a los migrantes sobre sus derechos, rutas seguras y mecanismos de denuncia disponibles.

Impacto positivo:

• Acceso inmediato a información sobre derechos humanos;

• Reducción de la desinformación y la vulnerabilidad;

• Inclusión lingüística y cultural;

• Protección de la dignidad y la seguridad personal.

4. Protección de las personas con discapacidad y accesibilidad tecnológica

Las personas con discapacidad aún enfrentan importantes barreras para acceder a la educación, el empleo, la justicia y los servicios públicos. La inteligencia artificial (IA) permite el desarrollo de soluciones inclusivas y accesibles, en consonancia con los principios de igualdad y no discriminación.

Ejemplo de aplicación en México (IA, inclusión y discapacidad):

El uso de sistemas de reconocimiento de voz, subtitulado automático y asistentes virtuales accesibles en plataformas institucionales facilita el acceso de las personas con discapacidades sensoriales a la información pública.

Por ejemplo, los portales digitales institucionales pueden integrar herramientas de traducción automática a lenguaje simplificado, audiodescripciones y contenido en Lengua de Señas Mexicana (LSM) mediante avatares digitales.

Impacto positivo:

• Acceso equitativo a la información pública;

• Inclusión digital efectiva;

• Fortalecimiento del principio de igualdad;

• Reducción de las barreras tecnológicas.

5. Proteger a las comunidades indígenas y reducir la brecha digital

Las comunidades indígenas en México constituyen un grupo particularmente vulnerable debido a las desigualdades históricas, el acceso limitado a los servicios y las barreras lingüísticas.

Ejemplo de aplicación en México (IA y derechos de los pueblos indígenas):

La inteligencia artificial puede utilizarse en plataformas educativas interculturales capaces de traducir automáticamente contenido sobre derechos humanos a lenguas indígenas como el náhuatl, el maya, el mixteco y el zapoteco.

Además, los sistemas de análisis de datos pueden identificar las áreas de mayor vulnerabilidad, lo que permite una focalización más eficaz de los programas educativos y las intervenciones de protección social.

Impacto positivo:

• Educación en derechos humanos culturalmente pertinente;

• Reducción de la exclusión lingüística;

• Fortalecimiento de la identidad cultural;

• Mayor eficacia de las políticas públicas inclusivas.

6. Protección de las personas mayores en contextos de vulnerabilidad social.

El envejecimiento de la población exige estrategias innovadoras para garantizar derechos fundamentales como la salud, la seguridad y el acceso a los servicios.

Ejemplo de aplicación en México (IA y derechos de las personas mayores):

Los sistemas de monitoreo inteligente integrados en programas sociales pueden

identificar situaciones de aislamiento, falta de acceso a servicios de salud o riesgo de exclusión económica.

Por ejemplo, una plataforma basada en IA puede notificar a las instituciones si una persona mayor no recibe atención médica, lo que permite implementar intervenciones de apoyo específicas.

Impacto positivo:

• Prevenir el abandono y el aislamiento social;

• Mejorar la atención sanitaria preventiva;

• Proteger el derecho a una vida digna;

• Optimizar los programas sociales.

7. Gobernanza ética de la inteligencia artificial

El uso de la inteligencia artificial en la protección de los derechos humanos debe regirse por los principios de legalidad, transparencia, protección de datos personales y no discriminación. En el contexto mexicano, esto implica alinear las soluciones tecnológicas con los marcos regulatorios nacionales y los estándares internacionales.

Ejemplo de aplicación en México (IA ética y derechos humanos):

La adopción de algoritmos verificables en los sistemas de asignación de asistencia social puede ayudar a prevenir sesgos discriminatorios y garantizar una distribución equitativa de los recursos basada en criterios objetivos.

Impacto positivo:

• Mayor equidad y transparencia en la toma de decisiones;

• Reducción de los sesgos institucionales;

• Fortalecimiento de la confianza pública;

• Protección integral de los derechos en el entorno digital.

Conclusión estratégica

La protección de los grupos vulnerables en México requiere una evolución institucional basada en la integración de tecnología, ética y derechos humanos. La inteligencia artificial, cuando se utiliza de forma responsable y estratégica, puede anticipar riesgos, ampliar el acceso a la justicia, personalizar las intervenciones educativas y fortalecer la inclusión social.

El impacto positivo es evidente: mayor eficiencia institucional, reducción de las desigualdades y una protección más efectiva de la dignidad humana. En el siglo XXI, la verdadera innovación se mide no solo por el progreso tecnológico, sino también por la capacidad de proteger a los más vulnerables. Desde esta perspectiva, la inteligencia artificial, guiada por un enfoque humanista, emerge como una herramienta esencial para construir una sociedad más justa, inclusiva y resiliente.

Capítulo 5

USO DE NUEVAS TECNOLOGÍAS EN LA ASESORÍA Y EL APOYO A LAS VÍCTIMAS

(Ignacio Domínguez)

Enfoque estratégico con Inteligencia Artificial y su impacto positivo en contextos críticos

El asesoramiento y el apoyo a las víctimas son funciones esenciales dentro del sistema de protección de los derechos humanos, especialmente en contextos críticos como la violencia de género, las violaciones de derechos fundamentales, el desplazamiento, la delincuencia, el abuso institucional y las crisis humanitarias. En la era digital, las nuevas tecnologías - en particular la inteligencia artificial (IA), las plataformas digitales, el análisis de datos y los sistemas automatizados de asistencia - están redefiniendo la forma en que las instituciones brindan orientación, apoyo psicológico, asesoramiento jurídico y seguimiento integral de las víctimas.

Desde una perspectiva tanto técnica como humanística, la tecnología no reemplaza el apoyo humano, sino que lo complementa, haciéndolo más accesible, oportuno, escalable y centrado en la dignidad de la persona, reduciendo así las barreras de acceso a la justicia y a los servicios de protección.

1. Asesoramiento jurídico digital asistido por inteligencia artificial.

El acceso a asesoría legal es una de las principales barreras para las víctimas, especialmente en contextos de vulnerabilidad económica, geográfica o social. La inteligencia artificial permite automatizar la orientación legal inicial, el análisis de casos y la identificación de posibles acciones institucionales.

Ejemplo de aplicación (inteligencia artificial en el asesoramiento jurídico a víctimas de violaciones de derechos humanos):

Una plataforma institucional basada en IA puede funcionar como un asistente legal digital que, mediante técnicas de procesamiento del lenguaje natural, analiza el relato de la víctima (denuncia, queja o testimonio) y clasifica el tipo de violación (discriminación, abuso de autoridad, violencia, omisión institucional).

El sistema puede sugerir vías legales, indicar las autoridades competentes, resaltar términos relevantes e identificar los derechos aplicables, de conformidad con los marcos regulatorios nacionales e internacionales.

Impacto positivo en contextos críticos:

• Acceso inmediato a asesoría jurídica, sin barreras geográficas;

• Reducción de los tiempos de respuesta institucionales;

• Fortalecimiento de la autonomía jurídica de la víctima;

• Mayor eficacia del derecho de acceso a la justicia.

2. Apoyo psicológico digital y asistencia emocional con IA.

Las víctimas de violencia, abuso o crisis humanitarias requieren apoyo emocional continuo y especializado. Las tecnologías basadas en inteligencia artificial permiten el desarrollo de sistemas digitales de apoyo psicológico accesibles y confidenciales.

Ejemplo de aplicación (inteligencia artificial en el apoyo emocional a las víctimas):

Un sistema de apoyo psicológico basado en IA puede ofrecer asistencia inicial continua (24/7) mediante chatbots entrenados en técnicas de primeros auxilios psicológicos, identificando crisis emocionales y derivando a las personas a especialistas.

La IA puede analizar patrones lingüísticos para detectar niveles de ansiedad, estrés postraumático o riesgo elevado, activando alertas automáticas para una intervención profesional oportuna.

Impacto positivo en contextos críticos:

• Disponibilidad inmediata de apoyo emocional;

• Reducción del aislamiento psicológico de la víctima;

• Identificación temprana de situaciones de crisis;

• Protección del derecho a la salud mental y a la dignidad personal.

3. Plataformas de denuncia digital y seguimiento inteligente de casos.

Muchas víctimas no denuncian por miedo, falta de información o dificultad para acceder a los canales oficiales. Las nuevas tecnologías permiten crear sistemas digitales seguros, incluso anónimos, para recibir y gestionar las denuncias.

Ejemplo de aplicación (IA en sistemas de informes digitales):

Una plataforma de denuncias con inteligencia artificial puede recibir informes en línea, verificar su coherencia, evaluar su urgencia y priorizar automáticamente los casos más graves (por ejemplo, situaciones de violencia extrema o que pongan en peligro la vida).

El sistema también puede generar un archivo digital rastreable, con monitoreo y actualizaciones automáticas sobre el estado del caso, lo que reduce el riesgo de revictimización institucional.

Impacto positivo en contextos críticos:

• Fortalecer la confianza en las instituciones;

• Incrementar las denuncias de violaciones de derechos;

• Mayor transparencia y trazabilidad de los procedimientos;

• Reducir la revictimización burocrática.

4. Soporte integrado mediante análisis predictivo.

La inteligencia artificial nos permite identificar factores de riesgo y diseñar programas de apoyo personalizados, especialmente en contextos de violencia doméstica, trata de personas o desplazamiento forzado.

Ejemplo de aplicación (IA en el monitoreo integrado de víctimas):

Un sistema institucional puede integrar datos sociales, psicológicos y legales relacionados con casos individuales (en cumplimiento de los principios de protección de datos) para elaborar perfiles de riesgo e identificar necesidades específicas.

Por ejemplo, en el caso de una víctima de violencia con antecedentes de reincidencia por parte del agresor y vulnerabilidad económica, el sistema puede recomendar la adopción de medidas de protección prioritarias, intervenciones de

apoyo social y asistencia jurídica reforzada.

Impacto positivo en contextos críticos:

• Protección preventiva y personalizada;

• Reducción del riesgo de reincidencia en la violencia;

• Un enfoque integral y multidisciplinario.

• Mayor eficacia de las políticas de protección.

5. Accesibilidad tecnológica para las víctimas en situación de vulnerabilidad.

Las víctimas que viven en zonas rurales, comunidades indígenas o contextos de exclusión social suelen enfrentarse a importantes obstáculos para acceder a los servicios institucionales. Las tecnologías digitales ayudan a reducir estas barreras.

Ejemplo de aplicación (IA multilingüe e inclusiva):

Los asistentes virtuales con inteligencia artificial pueden ofrecer asesoramiento en varios idiomas, incluyendo lenguas indígenas, a través de interfaces accesibles desde dispositivos móviles.

De esta manera, las víctimas pueden recibir información sobre sus derechos, mecanismos de denuncia y servicios disponibles sin necesidad de desplazarse físicamente.

Impacto positivo en contextos críticos:

• Inclusión lingüística y digital;

• Reducción de las barreras territoriales;

• Igualdad de acceso a los servicios de protección;

• Fortalecimiento del principio de no discriminación.

6. Uso de la inteligencia artificial en la protección de las víctimas de la ciberviolencia.

La ciberviolencia, el acoso en línea y la difusión ilegal de contenidos representan nuevas formas de agresión contra los derechos humanos.

Ejemplo de aplicación (inteligencia artificial en la protección contra la ciberviolencia):

Los sistemas de IA pueden monitorear entornos digitales para identificar contenido ofensivo, amenazas o divulgación no autorizada de datos personales, activando procedimientos de denuncia y eliminación.

Asimismo, las plataformas de soporte pueden ofrecer asesoramiento legal, ayuda para recopilar pruebas digitales y asistencia para presentar quejas.

Impacto positivo en contextos críticos:

• Proteger la identidad digital;

• Reducir los daños psicológicos y sociales;

• Responder con prontitud a los ataques en línea;

• Fortalecer el derecho a la privacidad y la seguridad digital.

7. Gobernanza ética y protección de datos

El uso de la tecnología en el asesoramiento y el apoyo a las víctimas debe cumplir con estrictos principios de confidencialidad, protección de datos personales, enfoque centrado en la persona y transparencia algorítmica.

Ejemplo de aplicación (IA ética en la gestión de casos):

Una plataforma institucional basada en IA puede integrar sistemas de anonimización, cifrado de datos y auditorías algorítmicas para garantizar la seguridad de la información y prevenir el uso indebido.

Estas medidas son especialmente relevantes en casos de violencia, abuso institucional o delitos graves, donde la protección de la víctima es una prioridad absoluta.

Impacto positivo en contextos críticos:

• Protección integral de la información sensible;

• Fortalecimiento de la confianza institucional;

• Prevención de filtraciones y violaciones de datos;

• Uso responsable y conforme a la normativa de la tecnología.

Conclusión estratégica

El uso de nuevas tecnologías en el asesoramiento y el apoyo a las víctimas representa una transformación estructural en los sistemas de protección de los derechos humanos. La inteligencia artificial permite intervenciones más rápidas, personalizadas y accesibles, especialmente en contextos críticos donde la puntualidad y la precisión de la acción institucional son cruciales.

Cuando se implementa con un enfoque ético, legal y humanista, la tecnología se convierte en una herramienta para la justicia, la protección y la empatía. Su impacto es significativo: mayor acceso a la justicia, mejor apoyo emocional, reducción de riesgos y fortalecimiento de la eficacia institucional.

En un futuro próximo, los sistemas de apoyo que integran la inteligencia artificial serán cada vez más capaces de garantizar una protección concreta, inclusiva y resiliente de los derechos humanos.

Capítulo 6

DERECHOS HUMANOS Y COMPUTACIÓN CUÁNTICA

(Ignacio Domínguez)

Convergencia estratégica entre inteligencia artificial, computación cuántica y la protección de la dignidad humana

La computación cuántica representa una de las tecnologías emergentes con mayor potencial transformador del siglo XXI. Su capacidad para procesar información mediante cúbits, superposición y entrelazamiento cuántico permite abordar problemas complejos con una velocidad y capacidad computacional potencialmente mayores que la computación clásica. En el ámbito de los derechos humanos, su integración con la inteligencia artificial abre un nuevo paradigma: sistemas predictivos, éticos y de alta precisión para la protección de la dignidad humana, la justicia, la inclusión y la gobernanza basada en la evidencia.

Desde una perspectiva de futuro, la computación cuántica no debe concebirse simplemente como una herramienta tecnológica avanzada, sino como un facilitador estratégico para fortalecer los sistemas de protección de los derechos humanos en contextos complejos, críticos y multidimensionales.

1. Protección del derecho a la privacidad y seguridad de los datos.

La privacidad es un derecho humano fundamental. Sin embargo, el avance de la computación cuántica presenta riesgos y oportunidades para la ciberseguridad y la protección de datos sensibles, especialmente en bases de datos de víctimas, organizaciones de derechos humanos y sistemas judiciales.

Ejemplo de aplicación: IA y computación cuántica en la protección de datos de víctimas

Un sistema institucional dedicado a los derechos humanos puede integrar la IA para gestionar archivos digitales y, al mismo tiempo, utilizar algoritmos de cifrado postcuántico resistentes a ataques cuánticos para proteger información altamente sensible, como denuncias, testimonios y datos biométricos.

La IA clasifica y anonimiza la información, mientras que el cifrado post-cuántico refuerza la protección de datos frente a futuras amenazas tecnológicas.

Impacto positivo:

• Mayor protección del derecho a la privacidad;

• Mayor seguridad de la información sensible;

• Prevención de fugas de datos y revictimización;

• Mayor confianza en los sistemas digitales dedicados a los derechos humanos.

2. Análisis predictivo de violaciones de derechos humanos mediante IA cuántica

Para prevenir las violaciones de derechos humanos se requieren modelos analíticos capaces de procesar variables sociales, económicas y territoriales complejas. La computación cuántica, combinada con la IA, permite la construcción de escenarios predictivos de mayor amplitud y precisión.

Ejemplo de aplicación: IA cuántica en el análisis de riesgos sociales

Un observatorio de derechos humanos puede utilizar algoritmos de aprendizaje automático acelerados cuánticamente para analizar grandes volúmenes de datos relacionados con indicadores de violencia, desigualdad, migración, pobreza y conflicto social.

De esta forma, el sistema puede identificar patrones recurrentes o difíciles de detectar con herramientas tradicionales, señalando áreas con alto riesgo de violaciones de derechos y facilitando intervenciones institucionales preventivas y políticas públicas específicas.

Impacto positivo:

• Prevención estructural de las violaciones de derechos humanos;

• Toma de decisiones basada en la evidencia;

• Optimización de las políticas sociales públicas;

• Protección temprana de las poblaciones vulnerables.

3. Acceso a la justicia y sistemas de justicia inteligentes

El acceso a la justicia es un derecho fundamental que puede fortalecerse mediante tecnologías avanzadas capaces de optimizar el análisis jurídico y la ge-

stión de casos complejos.

Ejemplo de aplicación: IA jurídica y computación cuántica

Un sistema de justicia inteligente puede utilizar la IA para analizar la jurisprudencia, los tratados internacionales y los precedentes legales, mientras que la computación cuántica puede ayudar a optimizar problemas complejos mediante simulaciones probabilísticas de escenarios jurídicos.

Esto permitiría priorizar los casos que implican violaciones de derechos humanos, identificar patrones de impunidad y reducir los tiempos procesales en las situaciones más críticas.

Impacto positivo:

• Mayor eficiencia judicial;

• Reducción de las demoras procesales;

• Mayor igualdad de acceso a la justicia;

• Fortalecimiento del estado de derecho.

4. Protección de grupos vulnerables mediante simulaciones cuánticas sociales

La computación cuántica permite simular sistemas sociales complejos, con posibles implicaciones para el diseño de políticas públicas inclusivas basadas en los derechos humanos.

Ejemplo de aplicación: IA y simulación cuántica en políticas sociales

Un modelo de simulación cuántica puede analizar el impacto de ciertas políticas públicas en comunidades vulnerables —niños, mujeres, migrantes o pueblos indígenas— mediante la integración de variables socioeconómicas, educativas y territoriales.

La IA puede interpretar los resultados del modelo y sugerir estrategias de intervención social dirigidas a reducir las desigualdades estructurales.

Impacto positivo:

• Diseñar políticas públicas más equitativas e inclusivas;

• Reducir las desigualdades sociales;

• Proteger específicamente a los grupos vulnerables;

• Planificar estratégicamente en función de escenarios complejos.

5. Derechos humanos, salud y medicina cuántica predictiva

El derecho a la salud puede fortalecerse mediante la convergencia de la IA y la computación cuántica, especialmente en la prevención de enfermedades y la optimización de tratamientos.

Ejemplo de aplicación: IA médica y computación cuántica

Los sistemas de IA integrados con algoritmos cuánticos pueden analizar grandes bases de datos biomédicas para detectar indicadores tempranos de enfermedades en poblaciones vulnerables.

En el contexto de la salud pública, la computación cuántica puede ayudar a modelar la propagación epidemiológica con mayor precisión, promoviendo estrategias preventivas y una distribución más eficiente de los recursos médicos.

Impacto positivo:

• Fortalecer el derecho a la salud;

• Diagnóstico precoz en poblaciones vulnerables;

• Optimizar los recursos sanitarios;

• Reducir los riesgos epidemiológicos.

6. Educación en derechos humanos mediante tecnologías cuánticas e IA

La educación es un derecho humano fundamental y constituye la base de sociedades justas e inclusivas. La computación cuántica puede impulsar plataformas educativas inteligentes y altamente personalizadas.

Ejemplo de aplicación: IA educativa y algoritmos cuánticos

Las plataformas educativas avanzadas pueden utilizar la IA para personalizar el contenido sobre derechos humanos y los algoritmos cuánticos para optimizar modelos de aprendizaje adaptativo a gran escala.

El sistema puede analizar el estilo cognitivo del usuario, su contexto sociocultural y su nivel educativo, ofreciendo cursos de formación accesibles sobre derechos humanos.

Impacto positivo:

• Democratizar el conocimiento sobre los derechos humanos;

• Educación personalizada y accesible;

• Reducir las desigualdades educativas;

• Fortalecer la cultura de la legalidad.

7. Gobernanza ética de la computación cuántica y derechos humanos

El desarrollo de la computación cuántica debe estar alineado con los principios éticos, regulatorios y de derechos humanos para prevenir riesgos como la desigualdad tecnológica, la vigilancia excesiva o la concentración del poder tecnológico.

Ejemplo de aplicación: IA ética y gobernanza cuántica

Un marco institucional puede integrar sistemas de auditoría algorítmica basados en IA para supervisar el uso responsable de las tecnologías cuánticas en las políticas públicas, garantizando la transparencia, la equidad y el respeto de los derechos fundamentales.

Además, los modelos cuánticos pueden utilizarse para evaluar el impacto regulatorio antes de la implementación de tecnologías disruptivas en sectores sensibles.

Impacto positivo:

• Uso responsable y ético de las tecnologías emergentes;

• Prevención de sesgos tecnológicos;

• Protección de las libertades fundamentales;

• Fortalecimiento de los marcos regulatorios de derechos humanos.

8. Ciberseguridad cuántica y la protección de los defensores de los derechos humanos

Los defensores de los derechos humanos suelen operar en entornos caracterizados por altos riesgos digitales. La computación cuántica aplicada a la ciberseguridad puede reforzar su protección tecnológica.

Ejemplo de aplicación: IA y criptografía cuántica para la protección de activistas.

Los sistemas de comunicación encriptados basados en técnicas resistentes a la computación cuántica, combinados con la monitorización de amenazas mediante IA, pueden proteger las comunicaciones de los defensores de los derechos humanos frente a ciberataques, espionaje digital o interceptación.

Impacto positivo:

• Protección de la libertad de expresión;

• Seguridad digital para defensores y organizaciones;

• Reducción del riesgo de vigilancia ilegal;

• Fortalecimiento de los ecosistemas democráticos.

Conclusión estratégica y visión de futuro

La convergencia de los derechos humanos, la inteligencia artificial y la computación cuántica representa un cambio de paradigma en la forma en que las instituciones pueden proteger la dignidad humana en la era tecnológica. Estas tecnologías nos permiten anticipar riesgos, optimizar las políticas públicas, fortalecer la justicia, proteger datos sensibles y garantizar los derechos fundamentales con niveles de precisión cada vez mayores.

Lejos de ser necesariamente una amenaza, la computación cuántica —si se implementa con una gobernanza ética y un enfoque humanista— puede convertirse en una herramienta estratégica para la protección integral de los derechos humanos. Su impacto positivo radica en su capacidad para abordar problemas complejos, reducir las desigualdades estructurales y construir sistemas institucionales más inteligentes, resilientes y centrados en las personas.

A medida que avanzamos en el siglo XXI, la verdadera innovación tecnológica será aquella que sitúe los derechos humanos en el centro del desarrollo cuántico y digital.

Capítulo 7

REFLEXIONES FINALES

(Marino Fardelli)

Las reflexiones que surgen de este trabajo conducen a una comprensión más profunda que la ya desarrollada. La transformación en curso no es meramente tecnológica ni exclusivamente organizativa, sino verdaderamente institucional.

La inteligencia artificial, junto con otras tecnologías emergentes, no solo impacta las herramientas de la acción administrativa; interviene, de manera más profunda, en las condiciones mismas del ejercicio del poder público. Los métodos de toma de decisiones están cambiando, los tiempos y los lugares de la relación entre la ciudadanía y la administración se transforman, y los límites entre discrecionalidad y automatización se redefinen. En este sentido, la cuestión tecnológica se convierte, en última instancia, en una cuestión de estabilidad del orden democrático.

En este contexto, el papel del Defensor del Pueblo ocupa una posición única y, en cierto modo, privilegiada. Al no estar sujeto a las rigideces de la acción administrativa ni a las formas del proceso judicial, conserva la flexibilidad institucional que le permite identificar tensiones sistémicas con antelación. Esta característica lo hace idóneo para desempeñar una función que, hoy más que nunca, resulta esencial: visibilizar lo que tiende a volverse invisible.

Si la burocracia tradicional se caracterizaba por un formalismo excesivo, la burocracia algorítmica corre el riesgo de producir un efecto opuesto, pero igualmente problemático: una aparente simplificación tras la cual se ocultan procesos de toma de decisiones complejos y de difícil acceso. Los ciudadanos ya no se enfrentan a un acto percibido como distante pero comprensible; se enfrentan cada vez más a un resultado que parece inmediato, pero cuyos determinantes son opacos.

Es precisamente en esta tensión entre simplificación y opacidad donde encaja la función de la defensa cívica. No se trata de oponerse a la innovación ni de frenar su progreso, sino de garantizar que no degrade progresivamente la acción pública. En otras palabras, la tarea no es detener el cambio, sino reconducirlo dentro de los límites legales y democráticos.

Desde esta perspectiva, la reflexión sobre la inteligencia artificial también exige una revisión del concepto mismo de rendición de cuentas pública. Mientras que

en el modelo tradicional la rendición de cuentas se centraba principalmente en el acto final, hoy tiende a distribuirse a lo largo de todo el ciclo de vida de los datos y las decisiones: desde la recopilación de información hasta su procesamiento, desde la configuración de algoritmos hasta la validación de resultados. La rendición de cuentas se vuelve así difusa, estratificada y organizativa, lo que requiere nuevas formas de control y nuevas herramientas de aplicación.

En este escenario, la defensa cívica está llamada a desempeñar una función que podríamos definir como "recomposición": tender puentes entre la toma de decisiones y la comprensión, entre la eficiencia y la justicia, entre la innovación y los derechos. Esta función no se limita a abordar casos individuales, sino que se extiende a la capacidad de interpretar los fenómenos en su dimensión sistémica, identificando los problemas críticos antes de que se traduzcan en conflictos generalizados.

Junto a esta dimensión institucional, emerge con fuerza una dimensión cultural. La integración de la inteligencia artificial en la administración pública no es solo una cuestión de regulaciones o tecnologías, sino de conciencia colectiva. Sin una comprensión adecuada de los mecanismos subyacentes a los sistemas digitales, el riesgo reside en la delegación involuntaria, en la que la aparente neutralidad de la máquina termina sustituyendo el juicio crítico humano.

Por ello, el desafío no solo concierne a los funcionarios públicos o a los profesionales del derecho, sino a toda la sociedad. Proteger los derechos en la era digital presupone una ciudadanía informada, instituciones transparentes y una cultura administrativa capaz de cuestionar la tecnología, sin someterse a ella.

De cara al futuro, parece claro que la cuestión central no será tanto la introducción de nuevas tecnologías, sino la capacidad de las instituciones para gestionar su impacto a lo largo del tiempo. La evolución de la inteligencia artificial, y aún más la de la computación cuántica, está destinada a acelerar aún más la complejidad de los sistemas de toma de decisiones. Desde esta perspectiva, el riesgo no reside en una sola tecnología, sino en la pérdida progresiva de control sobre los procesos que genera.

Aquí es donde entra en juego el papel del Defensor del Pueblo: no solo como salvaguarda, sino como garante del equilibrio entre innovación y derechos. Este equilibrio no se puede alcanzar de una vez por todas, sino que debe buscarse, adaptarse y verificarse constantemente a la luz de los cambios continuos.

Las páginas anteriores han mostrado cómo es posible imaginar un modelo de defensoría del pueblo capaz de acompañar la transición digital sin abandonar sus principios fundacionales. Estas reflexiones finales pretenden reiterar un punto clave: el futuro de los derechos no dependerá de la tecnología en sí mi-

sma, sino de la calidad de las instituciones responsables de su gestión.

En este sentido, el Defensor del Pueblo está destinado a seguir siendo una figura central. No porque sea inmune al cambio, sino precisamente porque es capaz de adaptarse a él manteniendo su función original: garantizar que, incluso en la era de los algoritmos, el individuo siga siendo el punto de referencia último para la acción pública.

Una sintesi schematica /

Un resumen esquemático

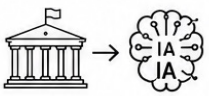
PRIMA PARTE

DIFESA CIVICA, TRASPARENZA E GOVERNANCE ALGORITMICA

L'ESPERIENZIA ITALIANA

La Prima Parte analizza come l'intelligenza artificiale e le tecnologie emergenti stanno trasformando la pubblica amministrazione italiana e il ruolo della Difesa Civica. Obiettivo centrale: garantire diritti, trasparenza ed equità nell'era digitale.

1 L'INTELLIGENZA ARTIFICIALE E LA PUBBLICA AMMINISTRAZIONE



IDEA CENTRALE

L'IA è già presente in molteplici processi della pubblica amministrazione italiana, offrendo opportunità ma anche rischi significativi.

APPLICAZIONI ATTUALI

- Redazione di documenti
- Classificazione e analisi delle informazioni
- Automatizzazione dei processi
- Gestione documentale
- Assistenza al cittadino

RISCHI CHIAVE

- "Shadow AI" e uso non supervisionato
- Fughe di dati e violazioni della privacy
- Bias e decisioni opache
- Delega informale di funzioni critiche
- Mancanza di trasparenza ed esplicabilità

2 SUPERARE LA CRISI DELLA GOVERNANCE

IDEA CENTRALE

La crisi di governance deriva dal divario tra la velocità tecnologica e la capacità regolatoria e istituzionale.

CAUSE PRINCIPALI

- La tecnologia avanza più velocemente delle leggi
- Opacità algoritmica
- Carenza di competenze digitali nelle istituzioni
- Disuguaglianza digitale
- Perdita di sovranità informativa

QUADRO DI RISPOSTA

- Regolazione come infrastruttura di fiducia
- Approccio alla gestione dei rischi sistemici
- Etica pubblica e innovazione responsabile
- Cooperazione tra istituzioni, esperti e cittadini

3 IL RUOLO DELLA DIFESA CIVICA

IDEA CENTRALE

Il Difensore Civico deve evolvere verso un ruolo strategico e predittivo per proteggere i diritti negli ecosistemi digitali.

NUOVE FUNZIONI

- Vigilanza e audit su algoritmi e decisioni automatizzate
- Garantire trasparenza ed esplicabilità
- Prevenire discriminazioni algoritmiche
- Proteggere persone e gruppi vulnerabili
- Mediazione tra cittadini, istituzioni e tecnologia

COMPETENZE NECESSARIE

- Conoscenze giuridiche
- Alfabetizzazione tecnologica
- Analisi dei dati
- Etica e diritti umani
- Visione interdisciplinare

4 DIFESA CIVICA E TRANSIZIONE DIGITALE

IDEA CENTRALE

La transizione digitale deve essere al servizio dei diritti e non al contrario.

LINEE GUIDA PER UNA TRANSIZIONE GIUSTA

- Tecnologia centrata sulle persone
- Inclusione e accessibilità digitale
- Protezione di dati e privacy
- Valutazione dell'impatto algoritmico
- Partecipazione civica attiva

STRUMENTI DI IA AL SERVIZIO DELLA DIFESA CIVICA

- Triage intelligente delle richieste
- Classificazione automatica dei casi
- Rilevazione di anomalie sistemiche
- Modelli predittivi di rischio
- Ricostruzione normativa automatizzata

5 CONSIDERAZIONI FINALI

IDEA CENTRALE

L'IA offre enormi possibilità, ma solo una governance responsabile e centrata sui diritti può garantire benefici reali e sostenibili.

MESSAGGI CHIAVE

- La tecnologia è uno strumento, non un fine.
- I diritti umani sono il limite e la bussola.
- Trasparenza e accountability sono indispensabili.
- La fiducia si costruisce con regole chiare, dati di qualità e controllo umano.
- La Difesa Civica è un pilastro per la democrazia digitale.

VISIONE

Costruire una pubblica amministrazione innovativa, trasparente, resiliente e al servizio di tutte le persone.

TEMI TRASVERSALI DELL'INTERA PRIMA PARTE

DIRITTI FONDAMENTALI
Al centro di ogni innovazione tecnologica.

TRASPARENZA ED ESPLICABILITÀ
Chiavi per la fiducia istituzionale.

EQUITÀ E INCLUSIONE
Evitare nuove forme di disuguaglianza ed esclusione digitale.

DATI E PRIVACY
Gestione responsabile e sovrana dei dati pubblici e personali.

GOVERNANCE MULTILIVELLO
Coordinamento tra Stato, regioni, agenzie e società civile.

INNOVAZIONE RESPONSABILE
Etica, legalità e tecnologia che lavorano insieme.

IN SINTESI

La Prima Parte mostra un percorso di evoluzione istituzionale:

COMPRENDERE
Le sfide dell'IA nella pubblica amministrazione.

→ **RICONOSCERE**
La crisi di governance e la necessità di nuove risposte.

→ **RAFFORZARE**
Il ruolo strategico del Difensore Civico.

→ **GUIDARE**
La transizione digitale mettendo al centro le persone e i loro diritti.

→ **GARANTIRE**
Una pubblica amministrazione giusta, trasparente e orientata al bene comune.

> "L'intelligenza artificiale non sostituisce la responsabilità pubblica; la rende più necessaria, più complessa e più umana."

SECONDA PARTE

INTELLIGENZA ARTIFICIALE IN FAVORE DELLA DIFESA CIVICA E DEI DIRITTI UMANI

DIRITTI UMANI E NUOVE TECNOLOGIE (PÁG. 35–66)

Le tecnologie emergenti, in particolare l'intelligenza artificiale, possono rafforzare la protezione, la promozione e la difesa dei diritti umani con un approccio etico, inclusivo e centrato sulle persone.

1 CAPITOLO 1

L'IA al servizio della difesa civica e dei diritti umani: diritti umani e nuove tecnologie.

IDEA CENTRALE

Le tecnologie ampliano opportunità e diritti, ma devono essere guidate da etica, legalità e dignità umana.

2 CAPITOLO 2

La difesa dei diritti e la sfida della cittadinanza digitale.

IDEA CENTRALE

La cittadinanza digitale richiede alfabetizzazione, partecipazione, responsabilità e inclusione per garantire diritti nell'era digitale.

3 CAPITOLO 3

Uso delle nuove tecnologie nella promozione ed educazione dei diritti umani in Messico.

IDEA CENTRALE

Le tecnologie possono educare, sensibilizzare e costruire cultura dei diritti con contenuti accessibili, innovativi e partecipativi.

4 CAPITOLO 4

Protezione dei gruppi vulnerabili.

IDEA CENTRALE

L'IA aiuta a identificare e proteggere i gruppi vulnerabili, ma è essenziale evitare discriminazioni e nuove esclusioni.

5 CAPITOLO 5

Uso di nuove tecnologie nella consulenza e nel sostegno alle vittime.

IDEA CENTRALE

Le tecnologie forniscono assistenza rapida, riservata e accessibile, migliorando l'accompagnamento e l'accesso alla giustizia.

6 CAPITOLO 6

Diritti umani e computazione quantistica.

IDEA CENTRALE

Il calcolo quantistico offre enormi potenzialità, ma solleva sfide etiche e di sicurezza che incidono sui diritti fondamentali.

7 CAPITOLO 7

Riflessioni finali.

IDEA CENTRALE

Tecnologia e diritti devono camminare insieme: etica, responsabilità, collaborazione e visione umanista.

PRINCIPI TRASVERSALI DI UN USO ETICO E UMANO DELLA TECNOLOGIA

DIGNITÀ UMANA

La persona è al centro: la tecnologia deve servire, non sostituire.

UGUAGLIANZA

Garantire accesso equo e non discriminatorio a tutti.

PRIVACY E SICUREZZA

Proteggere i dati personali e prevenire abusi e sorveglianza indebita.

TRASPARENZA

Algoritmi comprensibili, decisionali verificabili e spiegabili.

PARTECIPAZIONE

Coinvolgere persone e comunità nelle decisioni che le riguardano.

RESPONSABILITÀ

Chi sviluppa e usa la tecnologia deve rendere conto dei suoi impatti.

APPLICAZIONI E CONTRIBUTI DELL'IA ALLA DIFESA DEI DIRITTI UMANI

PROMOZIONE ED EDUCAZIONE

Creazione di contenuti, campagne digitali e piattaforme interattive per la cultura dei diritti.

RILEVAZIONE E MONITORAGGIO

Analisi dei dati per identificare violazioni, discriminazioni e tendenze emergenti.

PROTEZIONE DEI VULNERABILI

Sistemi predittivi per prevenire rischi e fornire risposte tempestive.

ASSISTENZA E SUPPORTO

Chatbot, assistenti virtuali e canali digitali per orientare e accompagnare le vittime.

ACCESSO ALLA GIUSTIZIA

Strumenti per semplificare procedure, documentare casi e garantire tracciabilità.

CITTADINANZA INCLUSIVA

Tecnologie accessibili per ridurre il divario digitale e favorire partecipazione.

SFIDE E RISCHI

- Divario digitale e nuove disuguaglianze.
- Bias algoritmici e discriminazioni.
- Mancanza di alfabetizzazione digitale.
- Minacce alla privacy e alla sicurezza.
- Uso improprio e sorveglianza di massa.

AZIONI RACCOMANDATE

- Rafforzare i quadri legali e le politiche pubbliche.
- Investire nell'educazione e nell'alfabetizzazione digitale.
- Promuovere etica, trasparenza e auditing algoritmico.
- Garantire la protezione dei dati e la sicurezza informatica.
- Favorire la cooperazione tra istituzioni, società civile e tecnologia.

IN SINTESI

L'intelligenza artificiale può essere una potente alleata dei diritti umani...

se usata con etica e responsabilità

se orientata alla giustizia e all'inclusione

se mette sempre al centro le persone

=

Difesa civica e diritti umani più forti, equi e sostenibili.

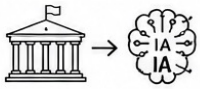
> "La tecnologia ha senso solo quando amplifica l'umanità, la libertà e la dignità di ogni persona."

PRIMERA PARTE

DEFENSA CÍVICA, TRANSPARENCIA Y GOBERNANZA ALGORÍTMICA

La Primera Parte analiza cómo la inteligencia artificial y las tecnologías emergentes están transformando la administración pública italiana y el papel de la Defensa Cívica. El objetivo central: garantizar derechos, transparencia y equidad en la era digital.

1 LA INTELIGENCIA ARTIFICIAL Y LA ADMINISTRACIÓN PÚBLICA



IDEA CENTRAL

La IA ya está presente en múltiples procesos de la administración pública italiana, ofreciendo oportunidades pero también riesgos significativos.

APLICACIONES ACTUALES

- Redacción de documentos
- Clasificación y análisis de información
- Automatización de procesos
- Gestión documental
- Atención al ciudadano

RIESGOS CLAVE

- "Shadow AI" y uso no supervisado
- Fugas de datos y privacidad
- Sesgos y decisiones opacas
- Delegación informal de funciones críticas
- Falta de transparencia y explicabilidad

2 SUPERAR LA CRISIS DE LA GOBERNANZA

IDEA CENTRAL

La crisis de gobernanza deriva de la brecha entre la velocidad tecnológica y la capacidad regulatoria e institucional.

CAUSAS PRINCIPALES

- Tecnología avanza más rápido que las leyes
- Opacidad algorítmica
- Falta de competencias digitales en las instituciones
- Desigualdad digital
- Pérdida de soberanía informativa

MARCO DE RESPUESTA

- Regulación como infraestructura de confianza
- Enfoque de gestión de riesgos sistémicos
- Ética pública e innovación responsable
- Cooperación entre instituciones, expertos y ciudadanía

3 EL PAPEL DE LA DEFENSORÍA CÍVICA

IDEA CENTRAL

El Defensor del Pueblo debe evolucionar hacia un rol estratégico y predictivo para proteger derechos en ecosistemas digitales.

NUEVAS FUNCIONES

- Vigilancia y auditoría de algoritmos y decisiones automatizadas
- Garantizar transparencia y explicabilidad
- Prevenir discriminaciones algorítmicas
- Proteger a las personas y grupos vulnerables
- Mediar entre ciudadanía, instituciones y tecnología

COMPETENCIAS NECESARIAS

- Conocimiento jurídico
- Alfabetización tecnológica
- Análisis de datos
- Ética y derechos humanos
- Visión interdisciplinaria

4 DEFENSA CÍVICA Y TRANSICIÓN DIGITAL

IDEA CENTRAL

La transición digital debe ponerse al servicio de los derechos y no al revés.

LINEAMIENTOS PARA UNA TRANSICIÓN JUSTA

- Tecnología centrada en las personas
- Inclusión y accesibilidad digital
- Protección de datos y privacidad
- Evaluación de impacto algorítmico
- Participación ciudadana activa

HERRAMIENTAS DE IA AL SERVICIO DE LA DEFENSA CÍVICA

- Triaje inteligente de solicitudes
- Clasificación automática de casos
- Detección de anomalías sistémicas
- Modelos predictivos de riesgos
- Reconstrucción normativa automatizada

5 CONSIDERACIONES FINALES

IDEA CENTRAL

La IA ofrece enormes posibilidades, pero solo una gobernanza responsable y centrada en los derechos puede garantizar beneficios reales y sostenibles.

MENSAJES CLAVE

- La tecnología es un medio, no un fin.
- Los derechos humanos son el límite y la brújula.
- La transparencia y la rendición de cuentas son indispensables.
- La confianza se construye con reglas claras, datos de calidad y control humano.
- La Defensa Cívica es un pilar para una democracia digital.

VISIÓN

Construir una administración pública innovadora, transparente, resiliente y al servicio de todas las personas.

TEMAS TRANSVERSALES DE TODA LA PRIMERA PARTE

DERECHOS FUNDAMENTALES
En el centro de toda innovación tecnológica.

TRANSPARENCIA Y EXPLICABILIDAD
Claves para la confianza institucional.

EQUIDAD E INCLUSIÓN
Evitar nuevas formas de desigualdad y exclusión digital.

DATOS Y PRIVACIDAD
Gestión responsable y soberana de los datos públicos y personales.

GOBERNANZA MULTINIVEL
Coordinación entre Estado, regiones, agencias y sociedad civil.

INNOVACIÓN RESPONSABLE
Ética, legalidad y tecnología trabajando juntas.

EN SÍNTESIS

La Primera Parte muestra un camino de evolución institucional:

COMPRENDER los desafíos de la IA en la administración pública.

→ **RECONOCER** la crisis de gobernanza y la necesidad de nuevas respuestas.

→ **FORTALECER** el papel estratégico del Defensor del Pueblo.

→ **GUIAR** la transición digital poniendo a las personas y sus derechos en el centro.

→ **GARANTIZAR** una administración pública justa, transparente y orientada al bien común.

> "La inteligencia artificial no reemplaza la responsabilidad pública; la vuelve más necesaria, más compleja y más humana."

SEGUNDA PARTE

INTELIGENCIA ARTIFICIAL EN FAVOR DE LA DEFENSA CÍVICA Y LOS DERECHOS HUMANOS

DERECHOS HUMANOS Y NUEVAS TECNOLOGÍAS

La Segunda Parte explora cómo las tecnologías emergentes, especialmente la inteligencia artificial, pueden fortalecer la protección, promoción y defensa de los derechos humanos, con un enfoque centrado en la ciudadanía, la inclusión y la ética.

1 CAPÍTULO 1

La IA en favor de la defensa cívica y los derechos humanos: Derechos humanos y nuevas tecnologías.

IDEA CENTRAL

Las nuevas tecnologías abren oportunidades para la defensa de los derechos humanos, pero deben estar guiadas por principios éticos, legales y centrados en la dignidad humana.

2 CAPÍTULO 2

La defensa de los derechos y el desafío de la ciudadanía digital.

IDEA CENTRAL

La ciudadanía digital implica nuevos derechos y responsabilidades. Es clave cerrar la brecha digital y garantizar la participación informada, segura e inclusiva.

3 CAPÍTULO 3

Uso de las nuevas tecnologías en la promoción y educación de los derechos humanos en el contexto mexicano.

IDEA CENTRAL

La tecnología puede potenciar la educación y cultura de derechos humanos mediante herramientas digitales accesibles, innovadoras y adaptadas a los contextos locales.

4 CAPÍTULO 4

Protección de grupos vulnerables.

IDEA CENTRAL

La IA puede ayudar a identificar riesgos, prevenir violaciones y diseñar políticas públicas más inclusivas para grupos en situación de vulnerabilidad.

5 CAPÍTULO 5

Uso de nuevas tecnologías en el asesoramiento y apoyo a las víctimas.

IDEA CENTRAL

Las tecnologías permiten brindar acompañamiento más rápido, eficiente y confidencial a las víctimas, facilitando el acceso a la justicia y la reparación.

6 CAPÍTULO 6

Derechos humanos y computación cuántica.

IDEA CENTRAL

La computación cuántica plantea enormes oportunidades y retos para la protección de datos, la seguridad y los derechos en la sociedad futura.

7 CAPÍTULO 7

Reflexiones finales.

IDEA CENTRAL

La tecnología debe estar al servicio de las personas y de los derechos humanos. El futuro exige ética, responsabilidad, colaboración y visión humanista.

PRINCIPIOS QUE ORIENTAN EL USO ÉTICO DE LA TECNOLOGÍA

DIGNIDAD HUMANA
Toda tecnología debe respetar y promover la dignidad de cada persona.

IGUALDAD Y NO DISCRIMINACIÓN
Evitar sesgos algorítmicos y garantizar inclusión y equidad.

PRIVACIDAD Y PROTECCIÓN DE DATOS
Garantizar el uso legítimo, seguro y transparente de la información.

TRANSPARENCIA Y EXPLICABILIDAD
Los sistemas deben ser comprensibles, auditables y responsables.

PARTICIPACIÓN Y EMPODERAMIENTO
Fomentar la participación ciudadana y el control democrático.

COOPERACIÓN Y SOLIDARIDAD
La protección de derechos requiere trabajo conjunto entre actores.

APLICACIONES DE LA IA Y TECNOLOGÍAS EMERGENTES EN LA DEFENSA DE DERECHOS

PROMOCIÓN Y EDUCACIÓN

- Plataformas educativas interactivas.
- Contenidos accesibles y multilingües.
- Difusión masiva y personalizada.

PROTECCIÓN E IDENTIFICACIÓN

- Análisis de datos para detectar riesgos.
- Sistemas predictivos para prevenir violaciones.
- Mapas y alertas tempranas.

ASESORAMIENTO Y APOYO

- Chatbots y asistentes virtuales.
- Orientación 24/7.
- Información clara sobre derechos y trámites.

ACCESO A LA JUSTICIA

- Herramientas para documentar casos.
- Gestión de expedientes digitales.
- Facilitación de denuncias y seguimientos.

INCLUSIÓN DIGITAL

- Reducir brecha digital.
- Tecnologías accesibles para todas las personas.
- Alfabetización digital como derecho.

RETOS PRINCIPALES

- Brecha digital y desigualdades estructurales.
- Sesgos algorítmicos y discriminación.
- Falta de marcos normativos adecuados.
- Riesgos para la privacidad y seguridad.
- Deshumanización y pérdida de control humano.

→

ACCIONES RECOMENDADAS

- Fortalecer marcos legales y políticas públicas.
- Invertir en educación digital y cultura de derechos.
- Garantizar transparencia, rendición de cuentas y auditoría.
- Promover investigación ética e innovación responsable.
- Colocar a las personas y sus derechos en el centro.

EN SÍNTESIS

La tecnología es una herramienta poderosa para la defensa de los derechos humanos. → Su uso debe ser ético, inclusivo y centrado en la dignidad humana. → La labor de las defensorías y la ciudadanía es clave para su buen uso. → Construir un futuro digital justo es responsabilidad de todas y todos.

La inteligencia artificial puede transformar la defensa de los derechos humanos, si la guiamos con ética, humanidad y visión de futuro.

DIFENSORE CIVICO della REGIONE LAZIO

CONSIGLIO REGIONALE DEL LAZIO