VADEMECUM PER L'IMPLEMENTAZIONE, L'USO ETICO E CONFORME DELL'INTELLIGENZA ARTIFICIALE NELLA PUBBLICA AMMINISTRAZIONE, AI FINI DEL RISPETTO DELLA PRIVACY

Sommario

Introduzione

L'implementazione dell'Intelligenza Artificiale impatta in maniera inevitabile e più o meno importante sulla corretta protezione dei dati personali, per questo è necessario che tutti gli operatori della Pubblica Amministrazioni siano consapevoli e formati nell'utilizzo dei nuovi strumenti informatici in particolare ai fini del rispetto della privacy e di tutte le norme a questa collegate.

Sezione I: La Missione dell'Ente Pubblico nell'era dell'IA

L'evoluzione tecnologica sta trasformando il panorama della Pubblica Amministrazione (PA), introducendo strumenti capaci di ottimizzare i processi e migliorare i servizi al cittadino. Tra questi, l'Intelligenza Artificiale (IA) rappresenta una delle frontiere più promettenti. Tuttavia, la sua adozione, spesso avvenuta in modo spontaneo e non regolato negli uffici pubblici, richiede una guida chiara e strutturata. Il presente vademecum è stato redatto con l'obiettivo di fornire un quadro operativo e normativo, delineando le buone pratiche e i comportamenti virtuosi che ogni dipendente dell'Ente è chiamato a rispettare per garantire un impiego dell'IA che sia al contempo innovativo, etico e conforme alla legislazione vigente.

1.1. L'Intelligenza Artificiale (IA): una Definizione per la Pubblica Amministrazione

Per comprendere l'ambito di applicazione di questo documento, è fondamentale partire da una definizione condivisa. Per "sistema di Intelligenza Artificiale" si intende un sistema automatico che, per obiettivi espliciti o impliciti, deduce dagli input ricevuti come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali. L'integrazione di questi sistemi nella PA mira a due obiettivi strategici principali: aumentare le capacità predittive per migliorare il processo decisionale basato sui dati e supportare la personalizzazione dei servizi pubblici, rendendoli più efficaci e, quando possibile, proattivi. Le finalità di miglioramento dei servizi e di riduzione dei costi sono, infatti, i principi guida che devono informare l'investimento in tecnologie di IA, consentendo di automatizzare compiti ripetitivi per liberare risorse da destinare alla qualità delle prestazioni.

1.2. Scopo e Ambiti del Vademecum

Questo documento si propone come uno strumento essenziale di governance, fornendo le indicazioni necessarie per l'adozione consapevole e regolamentata dell'IA. Il suo scopo è quello di tradurre le complesse prescrizioni normative in orientamenti pratici per tutti i dipendenti pubblici, in linea con i principi di: analisi del rischio, trasparenza, inclusività, accessibilità, privacy, sicurezza, formazione e sostenibilità. Delinea, inoltre, i diversi ambiti di applicazione, dalla gestione documentale ai servizi di interazione con i cittadini, e introduce le figure professionali e i ruoli che operano in questo nuovo ecosistema. La sua adozione è un passo cruciale per garantire che l'Ente operi nel rispetto dei diritti fondamentali della persona e mantenga la fiducia dei cittadini, prevenendo rischi e sanzioni derivanti da un uso improprio o non regolamentato.

Sezione II: Il Mosaico Normativo e le Direttive di Riferimento

L'utilizzo dell'intelligenza artificiale da parte di un'Amministrazione Pubblica non si sottrae al rispetto del quadro giuridico esistente, ma si inserisce in un contesto normativo complesso, che richiede un'analisi congiunta di diversi regolamenti e direttive. In particolare, il trattamento dei dati personali attraverso sistemi di IA è regolato da un'intersezione di norme europee e nazionali, che definiscono i confini entro i quali è possibile muoversi.

2.1. Il Pilastro della Protezione Dati: il Regolamento (UE) 679/2016 (GDPR)

Il GDPR stabilisce principi fondamentali e obblighi specifici che si applicano integralmente all'uso dell'IA nella PA, garantendo che ogni trattamento di dati personali avvenga su basi legali valide e trasparenti.

- **Principi Chiave del Trattamento:**
    - **Liceità, Correttezza e Trasparenza:** Il trattamento deve avere una base giuridica appropriata, come l'adempimento di un obbligo legale o l'esecuzione di un compito di interesse pubblico o l'esercizio di pubblici poteri. È essenziale che l'Ente fornisca agli interessati informazioni chiare e concise sugli scopi e le modalità di utilizzo dell'IA.
    - **Limitazione della Finalità e Minimizzazione dei Dati:** L'ente può raccogliere e utilizzare solo i dati strettamente indispensabili rispetto alle finalità definite, evitando trattamenti incompatibili con lo scopo originale della raccolta. L'identificazione accurata dei dati personali necessari e la pulizia degli stessi è un passaggio cruciale per evitare il rischio di *overfitting* e *underfitting* (*sovrallenamento e sottoallenamento*) del modello.
    - **Esattezza e Conservazione:** I dati personali devono essere esatti e aggiornati. L'Ente deve adottare misure ragionevoli per rettificare o cancellare tempestivamente dati inesatti e definire periodi di conservazione che non superino il tempo necessario per il raggiungimento delle finalità di trattamento.
- **Obblighi Procedurali Cruciali:**
    - **Valutazione d'Impatto sulla Protezione dei Dati (DPIA):** Laddove il trattamento di dati personali con l'IA comporti un rischio elevato per i diritti e le libertà delle persone fisiche, l'Amministrazione è obbligata a condurre una DPIA prima di avviare il trattamento.
    - **Diritti degli Interessati:** L'Ente deve implementare procedure per garantire l'effettivo esercizio di diritti come quello di accesso, rettifica, cancellazione, e in particolare, il diritto di ottenere l'intervento umano in caso di decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione.

2.2. Il Nuovo Quadro Giuridico: il Regolamento (UE) 2024/1689 (AI Act)

L'AI Act, primo quadro giuridico completo a livello globale sull'IA, non si sostituisce al GDPR ma lo integra, stabilendo un approccio basato sul rischio per l'immissione sul mercato

e l'utilizzo dei sistemi di IA. L'Ente deve comprendere e applicare questa classificazione a ogni sistema che intende adottare.

- **I Livelli di Rischio per un Ente:**
    - **Rischio Inaccettabile:** Sono proibiti tutti i sistemi che rappresentano una chiara minaccia ai diritti fondamentali. Un Ente non può in alcun modo utilizzare sistemi di *social scoring (punteggio sociale)*, di categorizzazione biometrica per dedurre caratteristiche protette o di *scraping (estrazione dati)* non mirato di contenuti web per la creazione di database di riconoscimento facciale.
    - **Rischio Elevato:** Rientrano in questa categoria i sistemi che possono causare un serio pregiudizio alla salute, alla sicurezza o ai diritti fondamentali. Esempi rilevanti per un'Amministrazione includono sistemi di IA utilizzati in: servizi essenziali (es. *credit scoring* per l'accesso a servizi pubblici), gestione del personale (es. *software* per la selezione di CV), o l'amministrazione della giustizia. I sistemi ad alto rischio sono soggetti a obblighi rigorosi: un'adeguata valutazione e mitigazione dei rischi, l'uso di dati di alta qualità, la registrazione automatica delle attività (*logging*), una documentazione dettagliata, una chiara informazione all'utilizzatore (*deployer*) e misure di supervisione umana.
    - **Rischio Limitato:** Riguarda i sistemi che necessitano di un'alta trasparenza, come i *chatbot* informativi o gli assistenti virtuali. L'obbligo principale per un Ente che li utilizza è quello di informare chiaramente l'utente che sta interagendo con una macchina e non con un essere umano.

La normativa AI Act introduce una distinzione formale tra il fornitore (*provider*), che sviluppa il sistema, e l'utilizzatore (*deployer*), che lo impiega. Nella stragrande maggioranza dei casi, l'Ente agirà come *deployer*, e questa qualifica comporta obblighi specifici che l'Ente non può delegare al fornitore. La responsabilità di garantire un'adeguata supervisione umana, la conservazione dei *log (file di registro)* e la trasparenza algoritmica ricade direttamente sull'Amministrazione. Ciò significa che l'Ente non può semplicemente accettare la certificazione di un fornitore, ma deve implementare un proprio sistema di governance e di controllo interno per assicurare la conformità del sistema durante tutto il suo ciclo di vita.

2.3. Trasparenza e Dati Aperti: il D.Lgs. 33/2013 e la Posizione di ANAC

L'obbligo di pubblicazione dei dati e dei documenti nella sezione "Amministrazione Trasparente" impone un'interessante riflessione in relazione all'IA. Molte Amministrazioni manifestano la preoccupazione che i dati pubblicati per legge possano essere raccolti attraverso *web scraping (estrazioni dal web)* per addestrare sistemi di intelligenza artificiale di terzi.

Tuttavia, il parere dell'Autorità Nazionale Anticorruzione (ANAC) del 30 gennaio 2025 ha chiarito in modo inequivocabile, in accordo con il Garante per la Privacy, che il decreto legislativo n. 33/2013 vieta espressamente all'Ente di applicare filtri o soluzioni tecniche che impediscano ai motori di ricerca di indicizzare ed effettuare ricerche all'interno della sezione "Amministrazione Trasparente". Questo perché la legge impone la totale accessibilità e

riutilizzabilità di tali dati. L'obbligo di trasparenza, dunque, prevale sulla preoccupazione di un utilizzo non voluto. La corretta condotta dell'Ente, in questo caso, non è quella di ostacolare l'accesso, ma di garantire che i dati pubblicati siano già conformi ai principi di minimizzazione e pertinenza, trattati nel rispetto della normativa sul riutilizzo dell'informazione del settore pubblico.

2.4. Le Linee Guida Nazionali: La Normativa Nazionale, AGID, ANAC e Garante Privacy

La Normativa Nazionale: Legge S1146-B approvata dal Senato il 17 settembre 2025, Disposizioni e deleghe al Governo in materia di intelligenza artificiale. Finalità e ambito di applicazione:

La Legge posiziona l'Italia come il primo Paese europeo a dotarsi di un quadro normativo organico in materia di Intelligenza Artificiale. L'obiettivo principale di questa legislazione è integrare e rafforzare le disposizioni del Regolamento europeo sull'IA (AI Act), adattandole al contesto istituzionale e sociale italiano, e promuovendo un modello di sviluppo "antropocentrico" in cui l'IA è al servizio della persona.

1. Principi e Scopo nella Pubblica Amministrazione

La legge interviene in modo specifico sull'uso dell'IA nella PA, ribadendo che il suo impiego deve servire a migliorare l'efficienza, ridurre i tempi dei procedimenti e aumentare la qualità e la quantità dei servizi offerti a cittadini e imprese. Un principio fondamentale stabilito dalla normativa è che l'IA deve agire come un "supporto decisionale tracciabile". La responsabilità finale, così come la decisione, deve sempre rimanere in capo a una persona fisica. Ciò significa che l'IA può fornire analisi e raccomandazioni, ma non può sostituire l'interpretazione umana, specialmente in ambiti delicati come l'attività giudiziaria, dove il magistrato conserva in ogni caso la prerogativa di applicare la legge e valutare i fatti.

2. Disposizioni Settoriali e Tutela dei Diritti

La legge delinea regole specifiche per l'applicazione dell'IA in vari settori, con un'attenzione particolare alla protezione dei diritti.

- **Lavoro e Personale**: I sistemi di IA utilizzati per la selezione, la valutazione e la gestione del personale rientrano nella categoria di "alto rischio" prevista dall'AI Act. Di conseguenza, l'utilizzo di tali sistemi implica un'attenzione particolare alla gestione del rischio, alla qualità dei dati e a misure per prevenire i *bias* (distorsioni) algoritmici. Inoltre, i datori di lavoro sono tenuti a informare i dipendenti sull'uso dei sistemi di IA.
- **Professioni Intellettuali**: Per professioni come quelle di avvocato o medico, la legge stabilisce che l'IA può essere utilizzata solo come supporto strumentale, e l'apporto intellettuale del professionista deve rimanere predominante. È inoltre obbligatorio informare il cliente in modo chiaro e semplice dell'utilizzo di sistemi di IA.
- **Sanità**: La legge consente la ricerca e la sperimentazione di sistemi di IA in ambito sanitario, anche con l'uso di dati sensibili, purché si rispettino i principi di *privacy by design* e minimizzazione dei dati.

3. Norme Penali e Protezione di Autore

La legge introduce specifici profili penali per contrastare l'uso illecito dell'IA.

- **Aggravante Penale**: Viene introdotta un'aggravante generica per i reati commessi con l'impiego di sistemi di IA, in particolare quando il sistema è utilizzato in modo insidioso.
- **Deepfake**: La normativa sanziona la diffusione illecita di *deepfake (immagini e audio falsati)*, con l'introduzione di pene detentive per chi utilizza l'IA per causare danno o per commettere crimini come frode o furto d'identità.

Per quanto riguarda il diritto d'autore, la legge riconosce la tutela delle opere dell'ingegno umano "create con l'ausilio dell'IA", a condizione che siano il risultato di un effettivo lavoro intellettuale dell'autore.

4. Governance e Competenze Nazionali

La legge attribuisce il ruolo di autorità nazionali competenti per la governance dell'IA ad AGID (Agenzia per l'Italia Digitale) e ACN (Agenzia per la Cybersicurezza Nazionale). Vengono, inoltre, fatte salve le competenze e i poteri del Garante per la Protezione dei Dati Personali e dell'Autorità Nazionale Anticorruzione (ANAC).

Oltre al quadro normativo europeo e nazionale, l'adozione dell'IA nella PA è supportata e vigilata da diverse autorità nazionali che forniscono direttive e orientamenti specifici.

- **AGID (Agenzia per l'Italia Digitale):** Svolge un ruolo centrale nella definizione della strategia nazionale sull'IA, pubblicando il Piano Triennale per l'Informatica nella PA. AGID ha anche redatto Linee Guida per l'adozione, l'acquisto e lo sviluppo di sistemi di IA, fornendo un pratico decalogo e indicazioni operative per le amministrazioni.
- **ANAC (Autorità Nazionale Anticorruzione):** L'Autorità si occupa della prevenzione della corruzione e della promozione della trasparenza, fornendo orientamenti sull'integrazione dell'IA nei processi di appalto pubblico.
- **Garante per la Protezione dei Dati Personali:** L'Autorità di controllo vigila sul rispetto del GDPR, fornendo pareri su decreti e provvedimenti che impattano sull'uso dell'IA, con un focus sul rispetto dell'etica, della dignità e della protezione dei dati personali.

Sezione III: Figure, Ruoli e Responsabilità nell'Ecosistema AI Pubblico

L'implementazione dell'IA in un'Amministrazione non è un compito che può essere affidato unicamente al dipartimento IT o al Responsabile per la Protezione dei Dati. La complessità normativa e tecnica richiede un approccio olistico e interdisciplinare, che coinvolga nuove figure professionali e una chiara ripartizione delle responsabilità.

3.1. Il Triumvirato di Ruoli Chiave: DPO, RTD e il Nascente CAIO

Il quadro normativo sull'IA, che interseca il GDPR con l'AI Act e le direttive nazionali, è talmente complesso che le figure tradizionali del Responsabile per la Protezione dei Dati (DPO)

e del Responsabile per la Transizione Digitale (RTD) devono essere affiancate da nuove competenze specialistiche.

Questa esigenza ha portato all'emersione di una nuova figura o di un team di lavoro dedicato, talvolta denominato Chief Artificial Intelligence Officer (CAIO), AI Compliance Officer o AI Risk Manager. Il CAIO funge da ponte tra l'innovazione tecnologica, la governance giuridica e l'operatività organizzativa. Il suo ruolo è complementare a quello del DPO e del RTD:

- **DPO:** Assicura la conformità al GDPR e l'effettivo esercizio dei diritti degli interessati. La sua consulenza è fondamentale nella conduzione delle DPIA e nella definizione della base giuridica del trattamento.
- **RTD:** Ha il compito di guidare l'ammodernamento tecnologico dell'Ente, definendo le strategie e coordinando l'integrazione dei sistemi.
- **CAIO (o team di compliance):** Si concentra sulla conformità specifica dell'IA, gestendo il rischio algoritmico e valutando i potenziali *bias (distorsioni)* e gli impatti sui diritti fondamentali. La sua funzione è quella di assicurare una conformità continua, gestendo le interazioni con i fornitori e con le autorità di vigilanza.

Questa sinergia è cruciale per garantire un approccio basato sulla gestione consapevole dei dati e un'analisi rigorosa dei rischi tecnologici. Il CAIO, lavorando insieme al DPO e al RTD, può assicurare un uso etico, trasparente e legittimo dei dati, proteggendo la fiducia dei cittadini e prevenendo effetti distorsivi come le discriminazioni algoritmiche.

Tavola 1: Mappa dei Livelli di Rischio AI Act per i Sistemi Pubblici

Categoria di Rischio	**Descrizione**	**Esempi di Uso in un Ente**	**Obblighi per l'Ente (Deployer)**
Inaccettabile	Sistemi considerati una chiara minaccia alla sicurezza e ai diritti fondamentali. Sono vietati.	*Social scoring*, riconoscimento biometrico in tempo reale in spazi pubblici.	Assoluto divieto di utilizzo.
Alto	Sistemi che possono comportare rischi gravi per la salute, la sicurezza o i diritti fondamentali.	Strumenti di selezione del personale, sistemi di gestione di servizi essenziali (es. assegnazione di benefici sociali), strumenti per l'amministrazione della giustizia.	Valutazione e mitigazione del rischio, conservazione dei log, documentazione dettagliata, supervisione umana, trasparenza, accuratezza e cybersicurezza.
Limitato	Sistemi che richiedono obblighi di trasparenza per	*Chatbot* informativi, assistenti virtuali.	Obbligo di divulgazione: l'utente deve essere informato che sta

Categoria di Rischio	Descrizione	Esempi di Uso in un Ente	Obblighi per l'Ente (Deployer)
	garantire la fiducia dell'utente.		interagendo con una macchina.
Minimo o Nullo	Sistemi che non presentano rischi significativi.	Applicazioni IA per videogiochi, filtri *spam*.	Nessun obbligo specifico previsto dall'AI Act.

3.2. La Responsabilità del Dipendente Pubblico nell'Uso dell'IA

L'uso di strumenti di IA da parte di un dipendente pubblico solleva importanti questioni in merito alla responsabilità per gli atti compiuti in violazione di diritti o che causano un danno. Ai sensi dell'articolo 28 della Costituzione e delle leggi applicabili, il dipendente pubblico è responsabile, secondo le norme penali, civili e amministrative, degli atti compiuti nell'esercizio delle sue funzioni.

Tuttavia, è cruciale distinguere tra le diverse forme di responsabilità:

- **Responsabilità Civile:** Riguarda i danni causati a terzi, esterni alla PA. In questo caso, il dipendente può essere chiamato a rispondere in solido con l'Ente.
- **Responsabilità Amministrativa:** Riguarda il danno patrimoniale arrecato alla stessa PA di appartenenza.
- **Responsabilità Disciplinare:** Si applica in caso di violazione di doveri d'ufficio, con sanzioni interne all'Amministrazione.

Un aspetto fondamentale, che attiene sia alla responsabilità amministrativa che a quella disciplinare, è che il dipendente risponde solo in caso di dolo (azione volontaria e consapevole) o colpa grave. La responsabilità è esclusa in caso di buona fede o colpa lieve. Questo principio sottolinea l'importanza cruciale della formazione e dell'adozione di protocolli operativi chiari. L'assenza di linee guida o la mancanza di formazione adeguata possono infatti rendere più difficile per l'Ente dimostrare che non vi è stata una condizione di colpa grave, esponendo sia l'Amministrazione che il dipendente a rischi maggiori.

Sezione IV: Strumenti e Applicazioni dell'IA a Disposizione dell'Ente

L'IA è già una realtà operativa nel settore pubblico. Comprendere le diverse soluzioni disponibili, sia a livello di strumenti per la comunicazione che di piattaforme per la gestione interna, è il primo passo per un'implementazione mirata ed efficace.

4.1. Chatbot e Assistenti Virtuali: la Frontiera della Comunicazione con il Cittadino

I *chatbot (robot conversazionali)* e gli assistenti virtuali rappresentano uno degli impieghi più diffusi dell'IA nella PA, offrendo un canale di comunicazione sempre attivo e

personalizzato. L'indagine di AGID ha rilevato che oltre il 60% dei progetti di IA nelle Amministrazioni centrali si basa su *chatbot* e assistenti virtuali.

Questi strumenti per la scrittura, il brainstorming, la sintesi e la risposta a domande complesse, sono tra i più diffusi sul mercato attuale:

Strumento	**Modello AI Utilizzato**	**Vantaggio Principale del Piano Gratuito**
Google Gemini	Gemini Pro	Profonda integrazione con l'ecosistema Google (Gmail, Drive) e accesso a informazioni in tempo reale.
ChatGPT	GPT-3.5	Il chatbot più diffuso e versatile; ottima per conversazioni, traduzioni e scrittura di base.
Microsoft Copilot	GPT-4 (e DALL-E 3)	Accesso a modelli GPT più avanzati di ChatGPT-free e generazione di immagini gratuita (tramite Bing Image Creator).
Perplexity	Modelli proprietari	Eccellente per la ricerca e l'analisi. Fornisce le fonti delle risposte, rendendole facilmente verificabili.
Mistral AI (Le Chat)	Mixtral	Offre accesso a uno dei modelli open-source più avanzati e performanti, con un focus sul rispetto degli standard europei.

4.2. Piattaforme per la Gestione Amministrativa e Documentale

L'IA generativa è già entrata negli uffici pubblici, spesso per iniziativa dei singoli dipendenti, e può essere utilizzata per semplificare compiti amministrativi e burocratici.

- **Focus sulla Community GenerativePA:** Un esempio di piattaforma specificamente pensata per la PA è GenerativePA, una *community* digitale. Il suo obiettivo è rendere l'IA "uno strumento di lavoro quotidiano" per l'Amministrazione, fornendo strumenti semplici e operativi per i dipendenti.
- **Casi d'Uso Pratici:** La piattaforma fornisce esempi concreti come la redazione di bozze di risposta a istanze comuni dei cittadini. Ad esempio, per rispondere rapidamente a 10 PEC su un argomento simile, un dipendente può inserire un *prompt* come "Scrivi una risposta istituzionale sull'applicabilità del contributo di costruzione in casi di ristrutturazione edilizia. Tono formale, valuta ogni caso singolarmente." L'IA genera una bozza personalizzabile, consentendo di risparmiare tempo e risorse.
- **Contenuti Formativi:** La piattaforma offre rubriche tematiche e contenuti come PilloleGenerative, video brevi sull'uso dell'IA, e Prompt della settimana, con suggerimenti pratici pronti all'uso.

Sezione V: Buone Pratiche e Misure Organizzative (Il Vademecum Pratico)

Per un corretto utilizzo dell'IA, l'Ente deve adottare un approccio sistemico e proattivo, che integri la conformità normativa nella struttura organizzativa e nella condotta di ogni singolo dipendente.

5.1. L'Approccio "by Design" (per progettazione) e "by Default" (per impostazione predefinita)

Le scelte architetturali e tecniche relative all'IA devono essere influenzate dalla necessità di integrare la protezione dei dati (*privacy by design*) e la conformità normativa fin dalla fase di progettazione e di scelta del sistema. Ciò implica l'adozione di misure tecniche e organizzative adeguate, come l'anonimizzazione e la pseudonimizzazione (fare in modo che i dati non siano direttamente riconducibili all'interessato) dei *dataset* (raccolta organizzata di dati) sensibili e l'implementazione di rigorosi sistemi di crittografia (rendere un messaggio comprensibile solo alle persone autorizzate). I dati di addestramento devono essere accuratamente puliti e monitorati regolarmente per garantirne la rilevanza e la protezione.

5.2. Trasparenza, Spiegabilità e Supervisione Umana

Un'implementazione etica e sicura dell'IA si basa su tre pilastri interconnessi:

- **Obbligo di Trasparenza:** L'Ente deve assicurare che gli utenti siano sempre informati in modo chiaro e comprensibile quando interagiscono con un sistema di IA, in particolare quando il sistema prende decisioni che li riguardano.
- **Spiegabilità:** Un sistema di IA, specialmente se ad alto rischio, deve essere sufficientemente interpretabile e spiegabile non solo dagli sviluppatori, ma anche da esperti esterni. Questo è cruciale per poter condurre audit (ispezioni) e verifiche in caso di malfunzionamenti o errori.
- **Supervisione Umana:** La normativa impone l'obbligo di garantire un livello adeguato di supervisione umana, specialmente per le decisioni ad alto impatto. I dipendenti devono avere la capacità di interpretare e, se necessario, invalidare gli *output (risultati)* del sistema, agendo come un filtro critico e responsabile.

5.3. La Valutazione d'Impatto Integrata (DPIA + FRIA)

L'adozione di un sistema di IA ad alto rischio richiede un'analisi del rischio approfondita e multidimensionale. L'AI Act richiede una *Fundamental Rights Impact Assessment (FRIA, Valutazione d'Impatto sui Diritti Fondamentali)* che deve essere condotta in parallelo alla DPIA del GDPR per garantire una valutazione olistica e completa.

Le Linee Guida di AGID fornisce uno strumento operativo fondamentale per questo processo, che va oltre la teoria e si traduce in una matrice di domande specifiche, obbligatorie e non, che l'Amministrazione deve porsi. Questa valutazione integrata deve considerare:

- L'impatto sui diritti fondamentali, verificando se l'uso del sistema è proporzionato rispetto all'impiego di tecnologie standard.
- La potenziale presenza di *bias (distorsioni)* indesiderati nei dati di *input* e *output*, con la necessità di adottare procedure per prevenirne la creazione o il rafforzamento.

- Il coinvolgimento e la consultazione degli *stakeholder* (portatori d'interessi come cittadini, dipendenti, autorità di vigilanza) fin dalle prime fasi di adozione.
- La robustezza tecnica del sistema, con la verifica di accuratezza, affidabilità e *cybersicurezza*.

5.4. Un Decalogo di Comportamenti Virtuosi per il Dipendente

Per orientare ogni dipendente verso un uso consapevole e conforme dell'IA, si riassumono di seguito le buone pratiche fondamentali da adottare quotidianamente.

Tavola 2: Decalogo di Comportamenti Virtuosi per il Dipendente Pubblico nell'Uso dell'IA

Azione Virtuosa	Motivazione
1. Verifica la base giuridica	Assicurati che l'uso dell'IA per il trattamento di dati personali abbia una base legale valida (es. interesse pubblico).
2. Usa solo i dati necessari	Applica il principio di minimizzazione: non inserire dati personali non indispensabili nei prompt (istruzioni) o negli input dei sistemi IA.
3. Informati sulla classificazione del sistema	Conosci il livello di rischio (Alto, Limitato, Minimo) del sistema che stai utilizzando, poiché a ogni categoria corrispondono obblighi specifici.
4. Non usare sistemi non autorizzati	Limita l'uso dell'IA a strumenti e piattaforme approvati dall'Ente per garantire sicurezza e conformità normativa.
5. Esercita la supervisione umana	Mantieni sempre un ruolo critico. Le decisioni ad alto impatto devono essere convalidate e, se necessario, modificate da un essere umano.
6. Non affidarti ciecamente all'output	Verifica sempre l'accuratezza, l'integrità e la coerenza degli output (risultati) generati dall'IA prima di utilizzarli in atti ufficiali o comunicazioni.
7. Sii trasparente con il cittadino	In tutte le interazioni che coinvolgono un sistema di IA, informa il cittadino che sta dialogando con una macchina.
8. Documenta ogni processo	Mantieni una documentazione chiara sull'uso del sistema e sulle decisioni prese, facilitando la tracciabilità e la responsabilità.
9. Partecipa alla formazione	L'IA e la normativa sono in continua evoluzione. Investi nella formazione continua per comprendere i rischi e le opportunità.

Azione Virtuosa	Motivazione
10. Segnala anomalie	Qualora rilevassi un malfunzionamento, un *bias (distorsioni)* o un'anomalia, segnalalo immediatamente alle figure preposte (RTD, DPO, team di compliance).

5.5. Come Elaborare dei Prompt Efficaci

Per scrivere dei prompt (istruzioni) efficaci all'IA, tali che ci permettano di ottenere le informazioni che cerchiamo, bisogna seguire delle tecniche specifiche o comunque avere alcuni accorgimenti che vengono di seguito riassunte.

Tavola 3: Istruzioni Operative per un Prompt Efficace

Titolo del Punto Chiave	Dettaglio (Cosa fare)
1. Sii Specifico e Dettagliato	Fornisci un obiettivo chiaro ed evita ambiguità. Indica precisamente cosa vuoi, invece di lasciare interpretazioni vaghe.
2. Definisci il Ruolo (Persona)	Chiedi all'IA di agire come un esperto (es. "un economista", "uno chef") per garantire una prospettiva e una qualità del contenuto adeguate.
3. Indica il Formato e la Struttura	Specifica la forma esatta dell'output che desideri: lista puntata, tabella, articolo con titoli H2, riassunto, codice, ecc.
4. Stabilisci il Tono e lo Stile	Definisci l'atteggiamento che il testo deve avere: formale, amichevole, professionale, ironico, accademico, in base al pubblico e allo scopo.
5. Usa Limitazioni e Contesti	Fornisci vincoli (es. "massimo 150 parole", "escludi il gergo tecnico") e tutte le informazioni di base che l'IA deve utilizzare per elaborare la risposta.

Conclusioni e Prospettive Future

L'implementazione dell'intelligenza artificiale non è un fine, ma un mezzo per modernizzare la PA e renderla più efficiente ed efficace al servizio dei cittadini. L'IA non è destinata a sostituire il dipendente pubblico, ma a diventare un prezioso alleato per automatizzare le attività routinarie e liberare tempo e risorse per compiti a maggior valore aggiunto.

Il successo di questa trasformazione, tuttavia, non dipende solo dalla tecnologia, ma da una governance (gestione) rigorosa che ne gestisca i rischi e ne garantisca l'uso etico e responsabile. La persona rimane al centro di questo processo, con il suo insostituibile ruolo di giudizio, validazione e supervisione. L'approccio olistico (globale), che integra protezione dei dati, trasparenza e analisi del rischio fin dalla fase di progettazione, è la chiave per costruire la fiducia dei cittadini e per trasformare le sfide normative in un'opportunità di crescita e innovazione sostenibile.

L'Ente si impegna a mantenere questo vademecum costantemente aggiornato, riconoscendo la natura dinamica della normativa e la necessità di un'evoluzione continua delle pratiche interne.