Digeat N.1 - 19 Marzo 2024

L’Intelligenza Artificiale nella PA: una nuova sfida per RTD e DPO

Di Anna Perut

Abstract

È recente la notizia della pubblicazione del Piano Triennale per l’Informatica nella Pubblica Amministrazione 2024-2026 da parte dell’Agenzia per l’Italia Digitale. Il Piano, che si discosta leggermente dalla struttura delle edizioni precedenti, affronta per la prima volta il tema dell’Intelligenza Artificiale, introducendolo come strumento determinante per migliorare l’efficienza e l’efficacia nella gestione e nell’erogazione dei servizi pubblici, e fornisce indicazioni e principi generali che dovranno essere adottati dalle amministrazioni nel prossimo triennio, tenendo in considerazione lo scenario normativo in rapida evoluzione. Ecco che allora la stretta interconnessione tra AI Act, normativa sulla protezione dei dati, cyber security, procurement, trasparenza, dati utilizzabili, imporrà agli RTD e ai DPO delle Pubbliche Amministrazioni l’obbligo di effettuare attente valutazioni per garantire l’adozione di tecnologie di intelligenza artificiale in modo consapevole ed efficace, portando efficienza ed innovazione nei servizi a favore dei cittadini. Alta formazione e aumento delle competenze appaiono quindi sempre più determinanti per gli attori coinvolti in prima persona nella realizzazione degli obiettivi prefissi da AgID, che saranno chiamati sempre di più ad un approccio sfidante multidisciplinare

Indice

Intelligenza Artificiale e Piano Triennale

L’Intelligenza Artificiale approda ufficialmente nella Pubblica Amministrazione. La nuova edizione del Piano Triennale per l’Informatica nella Pubblica Amministrazione 2024-2026 affronta per la prima volta il tema dell’Intelligenza Artificiale, introducendolo come strumento innovativo utile per migliorare l’efficienza e l’efficacia nella gestione ed erogazione dei servizi pubblici.

Il Piano, che presenta una struttura parzialmente diversa da quella delle edizioni precedenti, fornisce indicazioni e principi generali che dovranno essere adottati dalle amministrazioni nel prossimo triennio, tenendo in considerazione lo scenario normativo in rapida evoluzione, e s**uggerisce altresì strumenti che le PA potranno utilizzare come modelli di supporto e best practice per pianificare i propri interventi in ambito di AI**.

L’Intelligenza Artificiale viene introdotta nel Capitolo 5 dedicato ai Dati quale tecnologia potenzialmente in grado di:

- automatizzare le attività di ricerca e analisi di informazioni semplici e ripetitive, liberando tempo di lavoro per attività di maggior valore;
- aumentare le capacità predittive, migliorando il processo decisionale basato sui dati;
- supportare la personalizzazione dei servizi incentrata sull'utente, aumentando l'efficacia dell'erogazione dei servizi pubblici.

> Ad oggi vi sono già alcune amministrazioni che utilizzano applicazioni di machine learning e nei prossimi anni si prevede un aumento esponenziale dell'utilizzo di sistemi di Intelligenza Artificiale. La nuova edizione del Piano mette quindi nero su bianco alcuni principi e valutazioni che dovranno essere necessariamente effettuate dalle PA che intendano introdurre sistemi di AI o proseguirne nell'utilizzo.

Il contesto normativo

La conoscenza del panorama normativo europeo di riferimento, seppur non ancora definitivo ed in rapida evoluzione, è determinante.

Norma fondamentale sarà l'AI Act, ovvero il regolamento europeo sull'Intelligenza Artificiale, che ha **l'obiettivo primario di assicurare che i cittadini europei possano beneficiare di nuove tecnologie di AI sviluppate e operanti in conformità alla sicurezza, ai valori, ai diritti fondamentali e ai principi dell'Unione**.

Il Regolamento stabilisce **obblighi sia per gli utenti** che utilizzano i sistemi di AI sotto la propria autorità, **tra cui rientrano anche le Pubbliche Amministrazioni, sia per i fornitori dei sistemi stessi**, classificando (ad oggi) i rischi connessi all'utilizzo di AI in quattro differenti livelli: rischio inaccettabile (vietato), rischio elevato, rischio limitato e rischio minimo.

> Le PA sono tenute quindi ad adottare strumenti e metodologie per valutare correttamente i rischi sottesi all'acquisizione di sistemi di AI, in modo da attuare le prescrizioni dell'AI Act con cognizione di causa.

La proposta di Regolamento, nell'ultima formulazione, **prevede per i sistemi di AI ad alto rischio** (ovvero quelli che possono incidere sensibilmente sulla salute, sicurezza o sui diritti fondamentali dell'uomo) **una serie di prescrizioni in tema di valutazione del rischio**, che deve essere una costante di tutto il ciclo di vita della soluzione di AI, stabilendo obblighi precisi a cui sono soggetti i vari attori coinvolti in base al proprio ruolo, tra cui rientrano evidentemente anche le PA utilizzatrici di sistemi di AI. Solo per citarne alcuni, deve essere garantita **l'adozione di adeguate misure tecniche ed organizzative** che assicurino un utilizzo dell'applicativo conforme alle regole tecniche, la presenza di personale competente e formato in materia di AI, la massima trasparenza ed informativa verso l'utente finale (questo vale anche per i sistemi a rischio limitato), così come il monitoraggio continuo del funzionamento del sistema di IA. Per determinati sistemi, sarà obbligatorio effettuare una valutazione d'impatto sui diritti fondamentali.

All'IA Act si aggiungeranno anche le **norme tecniche europee sui sistemi di intelligenza artificiale in corso di elaborazione da parte degli Enti di normazione europei CEN e CENELEC**, nonché le tre Linee guida che AgiD sta predisponendo, volte rispettivamente a promuovere l'adozione dell'AI nella Pubblica Amministrazione, alla disciplina del procurement di AI e una dedicata allo sviluppo di applicazioni di AI per la PA, tutte di prossima adozione.

Le prospettive per gli RTD e i DPO

> In questo contesto i **Responsabili per la transizione al digitale e gli Uffici per la transizione al digitale avranno un ruolo determinante** e, quali attori principali, saranno tenuti ad ampliare le proprie conoscenze ed approfondire una materia ad oggi ancora poco conosciuta, in modo da assicurare la conformità normativa nel caso in cui l'ente di appartenenza decida di adottare sistemi di AI. Trattandosi di argomenti tecnici e complessi, sarà comunque auspicabile il supporto da parte di professionisti, anche esterni, qualificati nei vari ambiti coinvolti, dalla gestione delle soluzioni di AI, all'etica, alla cybersecurity.

L'approccio più critico riguarda evidentemente **i sistemi classificati ad alto rischio**, per i quali sono richieste valutazioni e adempimenti rigorosi. Per quanto sia ragionevole aspettarsi che, almeno in una prima fase, una buona parte delle applicazioni di AI presenteranno rischi limitati se non minimi (ad esempio chatbot, assistenti virtuali), è importante sensibilizzare gli RTD perché solo con l'approfondimento della normativa e dei relativi obblighi sarà possibile monitorare il livello di rischio dei propri sistemi per valutare, con consapevolezza, se sia necessario procedere con adempimenti ulteriori in modo da garantire la *compliance* ai requisiti del regolamento.

Anche il Piano stesso sottolinea in più riprese **l'importanza se non la necessità di promuovere la formazione e l'aggiornamento delle competenze all'interno delle Pubbliche Amministrazioni** in modo da impartire le conoscenze necessarie per la comprensione e gestione dell'AI.

Se gli RTD avranno un ruolo centrale nella pianificazione, nel procurement e nel monitoraggio dei sistemi, non si potrà non evidenziare come sia altrettanto determinante **l'adeguato e tempestivo coinvolgimento dei Responsabili della protezione dei dati,** in tutte le fasi di approvvigionamento. La *data protection* è un aspetto cardine dei sistemi di Intelligenza Artificiale, lo stesso AI Act contiene chiari riferimenti al Regolamento UE 679/16.

Il rispetto **dei principi di *privacy by design* e *by default***, l'adozione di misure di sicurezza tecniche ed organizzative adeguate a tutela dei diritti degli interessati non devono rimanere mere dichiarazioni di intenti ma essere declinate in modo effettivo nelle singole realtà.

Nella maggior parte dei casi **le Pubbliche Amministrazioni titolari del trattamento saranno tenute ad eseguire obbligatoriamente in modo preventivo la valutazione d'impatto sulla protezione dei dati sui trattamenti effettuati tramite sistemi di AI**, oppure, qualora ritengano che l'applicativo non comporti un rischio elevato nei trattamenti, dovranno giustificare la scelta di non eseguire la DPIA, nel rispetto dell'*accountability* (per quanto l'esecuzione della DPIA, ove non obbligatoria, rimanga comunque una buona pratica).

Tenuto conto delle possibili implicazioni dei sistemi di AI sarà quindi fondamentale considerare il possibile impatto non solo sui dati personali, ma anche sui **diritti fondamentali degli individui sanciti dalla Costituzione e dalle fonti europee e sovranazionali**, estendendo la valutazione, a seconda del contesto, anche al rispetto dei principi etici quali, ad esempio, l'assenza di discriminazioni e di distorsioni.

Ancora, in merito alla valutazione della necessità e proporzionalità del trattamento, bisognerà essere in grado di **dimostrare che l'utilizzo dell'AI sia la soluzione più adatta per perseguire la finalità concreta e che il trattamento sia comunque proporzionato**, bilanciando gli interessi del titolare del trattamento con i diritti e le libertà degli interessati e le loro ragionevoli aspettative. Alcuni spunti interessanti in materia vengono forniti dall'Information Commissioner's Officer – ICO (l'autorità di controllo inglese) nella sua "Guidance on AI and data protection".

La PA virtuosa dovrà quindi coinvolgere il DPO fin dalla fase embrionale affinché possa sorvegliare l'esecuzione della DPIA e fornire il proprio parere previsto dall'art. 39 GDPR, e non a sistema implementato.

Il ruolo del DPO in tutte le fasi dell'approvvigionamento digitale non è certo una novità, le attuali Linee Guida AgiD sulla sicurezza nel *procurement* affermano chiaramente che le PA devono porre attenzione alla protezione dei dati sia nella fase preliminare al *procurement* che in quella successiva alla stipula contrattuale, nel rispetto del principio di *accountability*, con il supporto del proprio DPO. La valutazione degli aspetti legati alla sicurezza e protezione dati deve tradursi anche nella **corretta definizione dei contenuti dei documenti di gara**, i quali devono individuare misure di sicurezza e ripartizioni di ruoli e responsabilità.

Nelle sue attività di sorveglianza il DPO sarà tenuto a verificare l'adempimento di tutti gli obblighi previsti dal GDPR correlati al sistema di AI, quali, solo per citarne qualcuno, la presenza di idonee informative sul trattamento dati, la corretta individuazione dei ruoli, le avvenute nomine a responsabile del trattamento ove necessarie, la formazione del personale, l'aggiornamento dei registri delle attività di trattamento.

Cosa fare nel frattempo? Un'occasione per migliorare l'accountability

> L'adozione di sistemi di AI, soprattutto negli enti di dimensioni medio piccole, verosimilmente richiederà del tempo. Lo stesso Piano AgID individua dicembre 2025 come primo orizzonte temporale di riferimento per l'adozione da parte delle PA delle Linee Guida AgID.

Nell'attesa della effettiva entrata in vigore della normativa **le PA potrebbero sfruttare questa finestra per svolgere un *assessment* della propria organizzazione e dei propri sistemi di gestione documentale e verificare il rispetto dei vari adempimenti previsti dal d.lgs. 82/2005 – CAD**, in modo da poter poi avviare il percorso di implementazione dell'AI partendo da un solido substrato in grado di sostenere le tecnologie innovative.