INNOVA JUS

RIVISTA MENSILE DEL CENTRO STUDI INNOVA JUS

ANNO I · NUMERO 2 · GIUGNO 2026

NUMERO MONOGRAFICO · IA E PUBBLICA AMMINISTRAZIONE

L'AMMINISTRAZIONE ALGORITMICA

L'intelligenza artificiale nella pubblica amministrazione: efficienza, garanzie, responsabilità

- La trilogia del Consiglio di Stato sull'algoritmo amministrativo
- L'art. 14 della legge 132/2025 e il modello italiano
- La PA come deployer dell'AI Act: obblighi e FRIA
- La sentenza CGUE Dun & Bradstreet (C-203/22): diritto all'esplicazione
- Profili operativi per dirigenti, DPO e Responsabile transizione digitale
- Le prospettive: dai decreti delegati alla governance integrata

CENTRO STUDI INNOVA JUS

Direttore scientifico: Prof. Avv. Michele Iaselli

innovajus.it

INNOVA JUS

Rivista mensile del Centro Studi Innova Jus

Anno I · Numero 2 · Giugno 2026

TESTATA

Innova Jus. Rivista mensile del Centro Studi Innova Jus.

DIREZIONE SCIENTIFICA

Prof. Avv. Michele Iaselli — Direttore del Centro Studi Innova Jus, docente di Informatica giuridica e Diritto dell'intelligenza artificiale presso LUISS Guido Carli e Università di Cassino, Coordinatore del Comitato Scientifico di Federprivacy.

TEMA DEL NUMERO

L'amministrazione algoritmica. L'intelligenza artificiale nella pubblica amministrazione: efficienza, garanzie, responsabilità.

PERIODICITÀ

Mensile. Ogni numero è dedicato a un argomento monografico di diritto dell'innovazione, con approfondimenti sistematici, ricognizione delle fonti primarie e profili operativi.

EDITORE

Centro Studi Innova Jus — Via Giovanni Merliani, 19 — 80127 Napoli (Italia). Sito: innovajus.it — Posta elettronica: info@innovajus.it

LINGUA

Italiano.

SUPPORTO E DIFFUSIONE

Edizione elettronica in formato PDF, diffusa gratuitamente sul sito dell'editore.

AVVERTENZA METODOLOGICA

Tutti i riferimenti normativi, gli atti istituzionali, le pronunce giurisprudenziali e le date richiamati nei contributi sono stati verificati su fonti ufficiali primarie (EUR-Lex per il diritto dell'Unione europea, Gazzetta Ufficiale e Normattiva per il diritto italiano, giustizia-amministrativa.it per la giurisprudenza del Consiglio di Stato, curia.europa.eu per la giurisprudenza della Corte di giustizia, garanteprivacy.it per i provvedimenti del Garante per la protezione dei dati personali). Eventuali profili in evoluzione sono espressamente segnalati come tali. Il fascicolo è chiuso alla data del 27 maggio 2026.

Sommario

EDITORIALE

L'amministrazione algoritmica

Tre fonti, un punto di equilibrio

di Michele Iaselli

L'apertura del numero precedente di questa rivista era dedicata a un'operazione di tecnica normativa europea — il Digital Omnibus — di cui si discuteva la portata sistematica. Il numero che il lettore ha tra le mani affronta una questione di pari rilievo, ma di segno diverso: non la riconfigurazione orizzontale di un corpo normativo già stratificato, bensì l'incontro tra una tecnologia in rapida evoluzione e l'architettura di garanzie che il diritto amministrativo italiano ha costruito nell'arco di oltre un secolo.

L'intelligenza artificiale nella pubblica amministrazione promette ciò che ogni innovazione amministrativa promette nel suo momento d'esordio: efficienza, riduzione dei tempi di definizione dei procedimenti, uniformità delle valutazioni, miglioramento della qualità dei servizi resi al cittadino. Sono promesse legittime e, se mantenute, di indubbio valore. Ma incontrano un nucleo duro: il rapporto tra l'amministrazione e il cittadino è un rapporto verticale di potere, governato da regole che ne organizzano la trasparenza, ne rendono sindacabile l'esercizio e, in ultima istanza, ne garantiscono la legittimazione democratica. Quando una decisione amministrativa è il prodotto, in tutto o in parte, di un'elaborazione algoritmica, quel rapporto cambia forma. Cambiano i flussi informativi tra amministrazione e cittadino, cambia il modo in cui si motiva la decisione, cambia l'oggetto stesso del sindacato giurisdizionale.

La tesi di questo numero, che attraversa tutti i contributi che seguono, è che il nostro ordinamento è oggi dotato — più di quanto a volte si dica — degli strumenti necessari per governare questo cambiamento. Tre fonti convergono nel disegnare un quadro coerente. La prima è la giurisprudenza del Consiglio di Stato, e in particolare la trilogia della sezione VI sull'algoritmo amministrativo: la sentenza n. 2270 dell'8 aprile 2019, le sentenze gemelle del 13 dicembre 2019 (n. 8472 in capo) e la n. 881 del 4 febbraio 2020. Da quel corpus emerge un orientamento sufficientemente stabile: l'algoritmo è un modulo organizzativo e strumento procedimentale, pienamente ammissibile anche nell'attività discrezionale, soggetto però alle verifiche tipiche di ogni procedimento e ai principi generali — conoscibilità, motivazione, tracciabilità — che il diritto amministrativo predica del provvedimento.

La seconda fonte è il Regolamento (UE) 2024/1689, l'AI Act, che disciplina la pubblica amministrazione in due qualità distinte: come destinataria di tutele rafforzate per il cittadino quando un sistema di IA incide su servizi pubblici essenziali (così esplicitamente il considerando 58), e come deployer di sistemi ad alto rischio, con gli obblighi che ne discendono — uso conforme alle istruzioni, sorveglianza umana, monitoraggio, valutazione d'impatto sui diritti fondamentali ex articolo 27. Lo slittamento delle scadenze applicative al 2 dicembre 2027 e al 2 agosto 2028, che il primo numero ha analizzato a fondo, non riduce la portata di questi obblighi: ne ridistribuisce l'orizzonte temporale.

La terza fonte è la legge 23 settembre 2025, n. 132, la prima disciplina organica italiana sull'intelligenza artificiale. Il suo articolo 14, dedicato specificamente alla pubblica amministrazione, prescrive che l'utilizzo dell'IA «avviene in funzione strumentale e di supporto all'attività provvedimentale, nel rispetto dell'autonomia e del potere decisionale della persona che resta l'unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata l'intelligenza artificiale». Non si tratta di una mera enunciazione di principio: è la traduzione legislativa, in chiave amministrativa, del principio della non esclusività della decisione automatizzata che il diritto europeo della protezione dei dati conosce dall'articolo 22 del GDPR e che la Corte di giustizia ha recentemente chiarito nella sentenza Dun & Bradstreet Austria del 27 febbraio 2025 (causa C-203/22), riconoscendo all'interessato il diritto a una

spiegazione concreta della logica seguita dal sistema.

Tre fonti, dunque, che parlano a registri diversi — giurisprudenziale, regolamentare europeo, legislativo nazionale — ma convergono su un punto: la decisione amministrativa, anche quando assistita dall'algoritmo, deve restare imputabile a un soggetto pubblico responsabile, comprensibile per chi ne è destinatario, sindacabile in sede giurisdizionale. È un punto di equilibrio impegnativo da mantenere nella pratica, perché ciascuno dei suoi elementi — imputabilità, comprensibilità, sindacabilità — richiede scelte organizzative, contrattuali e formative che spesso non sono state ancora compiute negli enti pubblici italiani.

I contributi che seguono cercano di dare conto di questo quadro nella sua articolazione concreta. Si apre con un inquadramento delle fonti a strati; si prosegue con il capitolo centrale sui principi della decisione amministrativa automatizzata; si analizza la pubblica amministrazione come deployer ai sensi dell'AI Act; si dedicano due contributi rispettivamente alle tutele del cittadino e ai profili operativi per chi nell'ente gestisce la conformità; chiude una nota prospettica sui decreti delegati che il Governo è chiamato ad adottare entro il termine di dodici mesi dall'entrata in vigore della legge 132/2025. Il fascicolo ospita inoltre un contributo specialistico, in via di pubblicazione, su un profilo che si è scelto deliberatamente di non trattare nei contributi redazionali per consentirne uno sviluppo più ampio.

Resta una considerazione di metodo, già enunciata nel primo numero ma che merita ribadire. In una materia in così rapido movimento, la tentazione del «sembra che» è permanente; abbiamo scelto di resisterle. Ogni riferimento normativo, ogni numero di articolo, ogni sentenza qui citata è stato verificato sulla fonte primaria ufficiale. Dove la verifica non è stata possibile, abbiamo omesso il dato anziché supplirlo con un'approssimazione. È una regola che costa più tempo di quanto possa sembrare; è anche, crediamo, la sola che renda utile per l'operatore una rivista che si dichiari scientifica.

INQUADRAMENTO

Le fonti a strati

Dal procedimento amministrativo classico all'AI Act e alla L. 132/2025

Il diritto applicabile all'uso dell'intelligenza artificiale da parte della pubblica amministrazione italiana non è contenuto in una fonte unica. È il prodotto di una stratificazione che, nel giro di poco più di un decennio, ha visto sovrapporsi norme costituzionali e amministrative classiche, regolazione europea della protezione dei dati, giurisprudenza amministrativa di legittimità, regolamentazione europea armonizzata sull'IA e, da ultimo, legislazione nazionale dedicata. La comprensione operativa del quadro richiede di tenere insieme questi diversi piani, evitando sia il riduzionismo che assume il solo AI Act come fonte rilevante, sia l'opposta semplificazione che continua a ragionare come se la dimensione europea fosse residuale.

Sul piano costituzionale e amministrativo classico, l'articolo 97 della Costituzione fissa il principio del buon andamento e dell'imparzialità dell'azione amministrativa; la legge 7 agosto 1990, n. 241, ne traduce le implicazioni in termini di trasparenza, motivazione, partecipazione e accesso. Questo strato non è una semplice cornice di sfondo: contiene i parametri di legittimità del provvedimento amministrativo, qualunque sia lo strumento istruttorio impiegato. Il Codice dell'amministrazione digitale (decreto legislativo 7 marzo 2005, n. 82) ha innestato su quel tronco la disciplina della digitalizzazione dell'azione amministrativa, fissando regole sulla validità degli atti, sull'identità digitale, sui servizi online, ma non ha originariamente affrontato la questione specifica della decisione automatizzata su base algoritmica.

Sul versante europeo della protezione dei dati, il Regolamento (UE) 2016/679 (GDPR) costituisce il primo testo che incide direttamente sui processi decisionali automatizzati attraverso l'articolo 22, che riconosce all'interessato il diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato che produca effetti giuridici o incida significativamente sulla sua persona. La pubblica amministrazione, in quanto titolare del trattamento, è pienamente vincolata da queste regole, fatte salve le condizioni che ne consentono la disapplicazione (consenso esplicito, esecuzione di un contratto, autorizzazione del diritto dell'Unione o dello Stato membro). La Corte di giustizia, con la recente sentenza del 27 febbraio 2025 nella causa C-203/22, Dun & Bradstreet Austria, ha chiarito che il diritto di accesso di cui all'articolo 15, paragrafo 1, lettera h, del GDPR comporta, in caso di processo decisionale automatizzato, il diritto dell'interessato a ottenere informazioni significative sulla logica utilizzata: il titolare deve descrivere la procedura e i principi concretamente applicati per produrre il risultato che ha investito l'interessato, in forma concisa, trasparente, intelligibile e facilmente accessibile.

La giurisprudenza amministrativa italiana ha sviluppato, in parallelo, un proprio orientamento. Il punto di partenza è la sentenza della Sezione VI del Consiglio di Stato dell'8 aprile 2019, n. 2270: la prima pronuncia in cui il giudice amministrativo si è confrontato con la legittimità dell'utilizzo di un algoritmo nell'ambito di una procedura amministrativa (un concorso docenti gestito tramite un sistema automatizzato di assegnazione delle sedi). Il Consiglio di Stato ha fissato in quella sede alcuni principi che sarebbero diventati il nucleo dell'orientamento successivo: i principi che informano l'attività amministrativa — trasparenza, partecipazione, conoscibilità, legalità — devono essere garantiti anche quando il procedimento è gestito da uno strumento automatizzato; l'algoritmo non può sostituire la valutazione discrezionale; deve restare possibile, per il cittadino e per il giudice, comprendere la logica seguita dal sistema.

La sentenza n. 8472 del 13 dicembre 2019 (presidente Montedoro, estensore Ponte), e le sue gemelle nn. 8473 e 8474 della stessa data, hanno ampliato significativamente quel quadro. Il Consiglio di Stato ha affermato che il ricorso all'algoritmo nel procedimento amministrativo è «pienamente ammissibile» e va inquadrato in termini di «modulo organizzativo, di strumento procedimentale ed istruttorio, soggetto alle verifiche tipiche di ogni procedimento

amministrativo, il quale resta il modus operandi della scelta autoritativa». Per la prima volta, il giudice amministrativo ha esplicitamente affermato che non vi sono ragioni di principio per limitare l'uso dell'algoritmo all'attività vincolata: anche l'attività discrezionale, a determinate condizioni, è compatibile con il supporto algoritmico, purché siano garantite la conoscibilità dell'algoritmo e l'imputabilità della responsabilità della decisione all'organo titolare del potere. La sentenza n. 881 del 4 febbraio 2020 ha confermato e consolidato questo orientamento, precisando ulteriormente la natura della «regola algoritmica» come regola amministrativa generale, costruita dall'uomo, e quindi soggetta ai principi generali dell'attività amministrativa, compresi quelli di pubblicità e trasparenza ai sensi degli artt. 1 e 8 della legge 241/1990.

Il Regolamento (UE) 2024/1689, l'AI Act, è la fonte più recente di questo edificio. Adottato il 13 giugno 2024 e pubblicato nella Gazzetta ufficiale dell'Unione europea del 12 luglio 2024, esso istituisce un quadro armonizzato basato sulla classificazione del rischio. Per la pubblica amministrazione, il Regolamento rileva sotto due profili tra loro intrecciati. Da un lato, classifica come ad alto rischio diversi sistemi di IA impiegati nei servizi pubblici: l'Allegato III individua espressamente i sistemi destinati a determinare l'accesso o l'ammissione a istituti di istruzione, quelli per la valutazione e selezione nel rapporto di lavoro, quelli usati dalle autorità pubbliche per valutare se concedere, negare, ridurre o revocare prestazioni essenziali di assistenza pubblica — sanità, sicurezza sociale, servizi sociali, assistenza abitativa — e quelli che intervengono nell'amministrazione della giustizia e nei processi democratici. Il considerando 58 è particolarmente esplicito sulla ratio di queste classificazioni: le persone che chiedono o ricevono prestazioni e servizi essenziali sono di norma in una posizione di vulnerabilità rispetto alle autorità responsabili. Dall'altro, il Regolamento impone agli utilizzatori di tali sistemi (deployer) un insieme di obblighi sostanziali che esamineremo nel contributo dedicato.

La legge 23 settembre 2025, n. 132 — pubblicata nella Gazzetta Ufficiale del 25 settembre 2025 ed entrata in vigore il 10 ottobre 2025 — chiude, allo stato, l'arco delle fonti rilevanti. Si tratta della prima disciplina organica italiana sull'intelligenza artificiale: 28 articoli, sei capi, un'architettura settoriale che dedica disposizioni specifiche al settore sanitario, al trattamento di dati personali, al lavoro, alle professioni intellettuali, alla pubblica amministrazione (articolo 14), all'attività giudiziaria (articolo 15), alla cybersicurezza nazionale. L'articolo 19 disciplina la Strategia nazionale per l'intelligenza artificiale e istituisce un Comitato di coordinamento presso la Presidenza del Consiglio; l'articolo 20 designa AgID e ACN come autorità nazionali responsabili dell'attuazione della normativa nazionale ed europea in materia di IA. L'articolo 24 reca una delega al Governo per l'adozione, entro dodici mesi dall'entrata in vigore della legge — dunque entro il 10 ottobre 2026 — di decreti legislativi di adeguamento al Regolamento (UE) 2024/1689 e di specificazione della disciplina dei casi di realizzazione e impiego illeciti di sistemi di IA. Quel termine è il prossimo orizzonte concreto entro cui il quadro nazionale sarà ulteriormente specificato.

DECISIONE AUTOMATIZZATA

I principi cardine

Non esclusività, conoscibilità, non discriminazione

Il principio della non esclusività della decisione automatizzata è oggi il cardine attorno a cui ruota la disciplina dell'amministrazione algoritmica nell'ordinamento italiano. Esso emerge in modo convergente, sebbene con sfumature diverse, da tutte le fonti rilevanti: la giurisprudenza amministrativa, il diritto europeo della protezione dei dati, la legge italiana sull'intelligenza artificiale, l'AI Act. Comprenderne la portata, e soprattutto le condizioni operative che ne consentono il rispetto effettivo, è la precondizione di qualsiasi corretta progettazione di un sistema di IA destinato a supportare l'azione pubblica.

La formulazione più nitida è oggi quella dell'articolo 14 della legge 132/2025. La disposizione stabilisce che l'utilizzo dell'intelligenza artificiale nella pubblica amministrazione «avviene in funzione strumentale e di supporto all'attività provvedimentale, nel rispetto dell'autonomia e del potere decisionale della persona che resta l'unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata l'intelligenza artificiale». Si tratta di un'enunciazione che condensa due principi distinti ma legati. Il primo è la strumentalità: il sistema di IA non è il decisore, è uno strumento istruttorio; il provvedimento amministrativo resta atto della persona fisica che lo adotta nell'esercizio del potere pubblico. Il secondo è l'imputabilità: la responsabilità del provvedimento, anche quando l'IA abbia contribuito in misura determinante alla sua formazione, è dell'organo titolare del potere; non vi è uno spazio in cui l'algoritmo «decida da sé» e sollevi l'amministrazione dalla responsabilità del proprio atto.

Questa formulazione recepisce, traducendolo nella lingua del diritto amministrativo, un principio che il diritto europeo della protezione dei dati conosce dal 2016. L'articolo 22, paragrafo 1, del Regolamento (UE) 2016/679 riconosce all'interessato il diritto a «non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona». Le eccezioni — consenso esplicito, esecuzione di un contratto, autorizzazione del diritto dell'Unione o dello Stato membro — non eliminano l'obbligo del titolare di assicurare misure appropriate per la tutela dei diritti, delle libertà e degli interessi legittimi dell'interessato, e in particolare il diritto di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione. La traiettoria interpretativa di questo articolo, lunga ormai un decennio, ha visto le autorità di controllo e le corti europee insistere sull'effettività del controllo umano: non basta una validazione formale, occorre un coinvolgimento sostanziale.

La sentenza della Corte di giustizia del 27 febbraio 2025, nella causa C-203/22, Dun & Bradstreet Austria, segna su questo punto un passaggio rilevante. La controversia originaria riguardava il rifiuto di un contratto di telefonia mobile motivato sulla base di una valutazione automatizzata del merito creditizio resa da una società specializzata. La cliente aveva chiesto, ai sensi dell'articolo 15, paragrafo 1, lettera h, del GDPR, di conoscere la logica utilizzata. La Corte ha affermato che, in caso di processo decisionale automatizzato ai sensi dell'articolo 22, paragrafo 1, l'interessato può pretendere dal titolare che gli sia spiegata, mediante informazioni pertinenti e in forma concisa, trasparente, intelligibile e facilmente accessibile, la procedura e i principi concretamente applicati per utilizzare, con mezzi automatizzati, i suoi dati personali al fine di ottenere il risultato che lo ha investito. La spiegazione deve essere tale da consentirgli di comprendere la decisione e, se del caso, di contestarla. La Corte ha specificato che questo non significa rivelare l'algoritmo nella sua interezza, in particolare quando si pongano esigenze di tutela del segreto commerciale: significa fornire una spiegazione operativa della logica seguita, sufficiente a permettere il sindacato sulla legittimità della decisione.

Per la pubblica amministrazione italiana, il riverbero di questa pronuncia è immediato. La motivazione del provvedimento amministrativo, prevista dall'articolo 3 della legge 241/1990, ha una funzione coincidente: rendere

comprensibile al destinatario il percorso logico-giuridico che ha condotto alla decisione, in modo da consentirne il sindacato. Quando una parte rilevante di quel percorso è gestita da un sistema di IA, l'obbligo di motivazione non si soddisfa con la mera indicazione che è stato utilizzato un algoritmo: occorre rendere conto della logica seguita, della rilevanza dei diversi input nell'esito, dei pesi attribuiti, delle ragioni della classificazione. È il punto su cui la giurisprudenza del Consiglio di Stato è stata, anche in questo, anticipatrice.

La sentenza della Sezione VI dell'8 aprile 2019, n. 2270, aveva fissato — pur con margini interpretativi — il principio della conoscibilità dell'algoritmo come condizione di legittimità del suo impiego. La sentenza n. 8472 del 13 dicembre 2019 ha dato a quel principio un fondamento più strutturato, agganciandolo al principio di trasparenza dell'azione amministrativa di cui all'articolo 1 della legge 241/1990 e al canone costituzionale del buon andamento di cui all'articolo 97 della Costituzione. La regola algoritmica — questa l'affermazione chiave della pronuncia, ripresa e consolidata dalla sentenza n. 881 del 4 febbraio 2020 — resta una regola amministrativa generale, costruita dall'uomo e applicata dalla macchina; conserva piena valenza giuridica e amministrativa anche quando viene declinata in forma matematica, e come tale deve soggiacere ai principi generali dell'attività amministrativa.

A fianco della non esclusività e della conoscibilità, il quadro contiene un terzo principio, quello della non discriminazione algoritmica. Esso ha una doppia radice. Sul versante della protezione dei dati, l'articolo 22 del GDPR, letto in combinato con il considerando 71, impone al titolare di utilizzare procedure matematiche o statistiche appropriate, di mettere in atto misure tecniche e organizzative adeguate al fine di garantire la rettifica dei fattori che comportano inesattezze, la minimizzazione del rischio di errori e l'impedimento di effetti discriminatori sulla base di caratteristiche protette. Sul versante dell'AI Act, l'articolo 10 sulla governance dei dati richiede ai fornitori di sistemi ad alto rischio di adottare appropriate misure di gestione dei dataset, comprese pratiche di analisi delle possibili distorsioni che possano pregiudicare la salute, la sicurezza o generare discriminazioni vietate dal diritto dell'Unione. Per la pubblica amministrazione che utilizzi sistemi di IA in funzioni sensibili — accesso a prestazioni, valutazione di personale, gestione di servizi sociali — questo profilo è di particolare rilievo: l'algoritmo che riproduce o amplifica una discriminazione storica non è un algoritmo neutrale, è un algoritmo difettoso, e il provvedimento che ne deriva è esposto a vizi di legittimità che il giudice amministrativo non avrà difficoltà a riconoscere.

Il quadro che ne risulta è impegnativo ma chiaro: il sistema di IA che assiste l'azione amministrativa deve essere strumentale e non sostitutivo, comprensibile nella sua logica, addestrato e validato su dati di qualità adeguata e tali da non riprodurre discriminazioni vietate, e in ogni caso accompagnato da una decisione umana effettiva, non meramente cerimoniale, da parte dell'organo titolare del potere. Sono condizioni che non si soddisfano con dichiarazioni di principio: richiedono scelte organizzative, contrattuali e formative che il prossimo contributo affronta dal punto di vista dell'amministrazione come utilizzatrice di sistemi ad alto rischio ai sensi dell'AI Act.

AI ACT

La PA come deployer

Allegato III, obblighi dell'articolo 26 e valutazione d'impatto sui diritti fondamentali

L'AI Act qualifica come «deployer» chiunque utilizzi un sistema di intelligenza artificiale sotto la propria autorità, con la sola esclusione dell'utilizzo nel corso di un'attività personale non professionale. Le pubbliche amministrazioni, quando impiegano sistemi di IA per assolvere ai propri compiti istituzionali, sono deployer a tutti gli effetti, e quando il sistema utilizzato rientra nelle categorie ad alto rischio dell'Allegato III, agli obblighi generali si aggiunge un complesso di obblighi specifici che disegnano un vero e proprio statuto del deployer pubblico.

La premessa è che molti dei sistemi di IA pertinenti all'azione amministrativa rientrano nell'Allegato III. La classificazione di un sistema come ad alto rischio non dipende dalla denominazione che il fornitore gli attribuisce, né dalla sofisticazione tecnologica, bensì dal contesto d'uso e dall'impatto potenziale sui diritti fondamentali, sulla salute o sulla sicurezza delle persone. L'Allegato III individua otto aree, di cui almeno quattro sono di evidente interesse per la pubblica amministrazione: i sistemi biometrici (lasciati salvi i sistemi di verifica per l'accesso a servizi); le infrastrutture critiche; l'istruzione e la formazione professionale, in particolare per la determinazione dell'accesso e dell'ammissione e per la valutazione dei risultati; l'occupazione e la gestione dei lavoratori, ivi compresi il monitoraggio e la valutazione delle prestazioni. Vi sono poi i sistemi utilizzati per determinare l'accesso a prestazioni e servizi essenziali — il considerando 58 menziona espressamente i servizi sanitari, le prestazioni di sicurezza sociale, i servizi sociali, l'assistenza abitativa — e quelli impiegati nelle attività di contrasto, nella migrazione, nella giustizia e nei processi democratici. La PA italiana, nei suoi diversi livelli e nelle sue diverse articolazioni, opera in ciascuna di queste aree.

Gli obblighi del deployer di sistemi ad alto rischio sono dettagliati dall'articolo 26 del Regolamento. Il primo nucleo riguarda l'uso conforme: il sistema deve essere utilizzato secondo le istruzioni d'uso fornite dal produttore. La sorveglianza umana deve essere assegnata a persone fisiche dotate di competenza, formazione e autorità adeguate, oltre che del supporto necessario. Sui dati di input, nella misura in cui il deployer ne controlla la selezione, sussiste l'obbligo di assicurare che essi siano pertinenti e sufficientemente rappresentativi rispetto alla finalità prevista. Il funzionamento del sistema deve essere monitorato secondo le istruzioni d'uso, e qualora il deployer abbia ragione di ritenere che l'uso conforme possa nondimeno generare un rischio ai sensi dell'articolo 79, paragrafo 1, è tenuto a informare senza indebito ritardo il fornitore o distributore e la pertinente autorità di vigilanza del mercato, sospendendo l'uso del sistema. Conservazione dei log, informazione delle persone interessate dalle decisioni assistite dall'IA, cooperazione con le autorità competono parimenti al deployer.

L'obbligo che concerne più direttamente la pubblica amministrazione è quello previsto dall'articolo 27: la valutazione d'impatto sui diritti fondamentali, nota nella prassi internazionale come FRIA (Fundamental Rights Impact Assessment). Il deployer pubblico di un sistema di IA ad alto rischio, prima di metterlo in uso, è tenuto a condurre una valutazione strutturata che individui i processi del deployer in cui il sistema sarà utilizzato, il periodo e la frequenza d'uso, le categorie di persone fisiche e i gruppi che ne saranno interessati, i rischi specifici di pregiudizio per essi, le misure di sorveglianza umana, le misure da adottare in caso di concretizzazione dei rischi, i meccanismi di governance interna. La FRIA non è una formalità documentale: è il punto in cui l'amministrazione, prima di esporre il cittadino agli effetti di un sistema, mette per iscritto le ragioni per cui ritiene che quel sistema possa essere utilizzato in modo legittimo, equo e proporzionato. È inoltre l'oggetto di una notifica all'autorità di vigilanza del mercato.

L'articolo 27, paragrafo 4, contiene un raccordo di rilievo operativo: se uno qualsiasi degli obblighi previsti dalla FRIA è già rispettato mediante la valutazione d'impatto sulla protezione dei dati effettuata a norma dell'articolo 35 del GDPR (o dell'articolo 27 della direttiva 2016/680), la FRIA integra tale valutazione anziché duplicarla. Il messaggio

per la PA italiana è chiaro: la FRIA non sostituisce la DPIA né viceversa, ma le due valutazioni vanno costruite in modo coordinato, e laddove la DPIA copra già alcuni profili della FRIA può essere richiamata o integrata. Per un'amministrazione che già conduce DPIA strutturate, l'estensione metodologica alla FRIA è un investimento incrementale; per un'amministrazione che non lo fa, il nuovo obbligo richiede di costruire da zero una capacità valutativa che è bene avviare con largo anticipo rispetto al 2 dicembre 2027.

A questi obblighi si aggiunge la registrazione nella banca dati dell'UE prevista dall'articolo 49 del Regolamento, che concerne i deployer pubblici (le autorità pubbliche o le istituzioni, gli organi e gli organismi dell'Unione, o chi agisce per loro conto) prima della messa in servizio o dell'uso di un sistema di IA ad alto rischio. È previsto un obbligo informativo verso le persone interessate da decisioni prese o assistite dal sistema, secondo le regole proprie del diritto dell'Unione e nazionale. Particolari obblighi informativi si applicano nel contesto lavorativo, dove il deployer è tenuto a informare i rappresentanti dei lavoratori e i lavoratori interessati prima della messa in uso.

Una specifica annotazione merita l'articolo 4 sull'alfabetizzazione in materia di IA, su cui il Digital Omnibus on AI è recentemente intervenuto ridimensionandone alcuni profili. Per i sistemi ad alto rischio l'obbligo a carico dei deployer di garantire un livello adeguato di alfabetizzazione del personale che opera con tali sistemi è confermato. Per la pubblica amministrazione italiana, questo significa che la formazione del personale che utilizza, supervisiona o si interfaccia con sistemi di IA ad alto rischio non è un'opzione: è una condizione di legittimità dell'uso. L'investimento formativo va dimensionato sulla complessità del sistema, sul livello di esposizione del personale e sull'impatto delle decisioni assistite sui destinatari.

In sintesi: l'amministrazione pubblica che oggi pianifica l'introduzione di sistemi di IA in funzioni sensibili deve costruire, in parallelo, quattro cantieri operativi — mappatura dei sistemi e classificazione del rischio; predisposizione metodologica della FRIA in raccordo con la DPIA; progettazione organizzativa della sorveglianza umana effettiva; formazione del personale. Sono cantieri che richiedono mesi di lavoro, non settimane; e le scadenze del 2 dicembre 2027 per i sistemi stand-alone e del 2 agosto 2028 per quelli incorporati in prodotti, fissate dall'accordo politico sul Digital Omnibus on AI del 7 maggio 2026, non sono lontane quanto possa sembrare.

TUTELE

Il punto di vista del cittadino

Motivazione, accesso, sindacato giurisdizionale, intervento umano

Il quadro normativo che abbiamo ricostruito si guarda dal punto di vista dell'amministrazione, ma esiste anche un altro punto di osservazione, complementare e altrettanto rilevante: quello del cittadino che è destinatario di un provvedimento amministrativo formato con il concorso, in misura più o meno determinante, di un sistema di intelligenza artificiale. Questo numero ha scelto di dedicargli un contributo distinto perché le tutele del cittadino non sono semplici proiezioni speculari degli obblighi dell'amministrazione: hanno una loro autonomia concettuale e una loro effettività che richiede attenzione specifica.

La cornice generale è offerta dal Regolamento (UE) 2024/1689, che colloca il «diritto a una buona amministrazione» tra i diritti fondamentali la cui salvaguardia giustifica la classificazione di taluni sistemi di IA come ad alto rischio (così, esplicitamente, il considerando 48). È un riferimento di grande rilievo concettuale: il Regolamento europeo riconosce che esiste un diritto del cittadino a un'amministrazione corretta, e che l'introduzione di sistemi di IA nell'azione pubblica può incidere su tale diritto al punto da richiedere una disciplina specifica. Sul piano del diritto positivo, questo diritto si articola in più posizioni soggettive che richiamano tradizioni giuridiche consolidate: il diritto a una motivazione adeguata del provvedimento, il diritto di accesso agli atti, il diritto a un ricorso effettivo e a un giudice imparziale.

Il primo profilo concerne la motivazione. La motivazione del provvedimento amministrativo è prevista, nell'ordinamento italiano, dall'articolo 3 della legge 7 agosto 1990, n. 241: l'atto deve indicare i presupposti di fatto e le ragioni giuridiche che ne hanno determinato l'adozione, in relazione alle risultanze dell'istruttoria. Quando una parte rilevante dell'istruttoria è gestita da un sistema di IA, l'obbligo di motivazione non si soddisfa con il mero richiamo all'esito dell'elaborazione algoritmica. Deve essere reso conto della logica seguita dal sistema, del modo in cui i diversi elementi sono stati valutati, delle ragioni per cui il caso del singolo è stato classificato in un determinato modo. Su questo punto convergono il principio di trasparenza dell'azione amministrativa, la giurisprudenza del Consiglio di Stato sulla conoscibilità dell'algoritmo e l'interpretazione che la Corte di giustizia ha dato del diritto di accesso ex articolo 15 del GDPR nella sentenza Dun & Bradstreet Austria del 27 febbraio 2025: il cittadino ha diritto a una spiegazione che gli consenta di comprendere la decisione e, ove ritenga di farlo, di contestarla.

Il secondo profilo concerne il diritto di accesso e l'esercizio del diritto di difesa. La legge 241/1990 disciplina il diritto di accesso agli atti del procedimento amministrativo; il decreto legislativo 14 marzo 2013, n. 33, ne integra la disciplina con il regime dell'accesso civico generalizzato. Sul versante della protezione dei dati personali, l'articolo 15 del GDPR riconosce all'interessato il diritto di accesso ai propri dati e, nei casi di decisione automatizzata, alle informazioni significative sulla logica utilizzata. Per il provvedimento amministrativo formato con il supporto di un sistema di IA, l'esercizio congiunto di queste posizioni soggettive — accesso amministrativo e accesso ex GDPR — consente al cittadino di acquisire un quadro adeguato a contestare la decisione. È un punto operativo di prima rilevanza per chi assista cittadini destinatari di provvedimenti adottati con il supporto algoritmico: la doppia base normativa rafforza la posizione e amplia le possibilità di documentazione.

Il terzo profilo è il sindacato giurisdizionale. La giurisprudenza del Consiglio di Stato cui si è già fatto riferimento — la trilogia 2270/2019, 8472/2019, 881/2020 — è stata costruita proprio nell'esercizio del sindacato di legittimità su provvedimenti adottati mediante algoritmo. Il giudice amministrativo ha mostrato di poter pienamente esercitare il proprio sindacato anche su decisioni algoritmiche, a condizione che la regola tecnica sia stata resa conoscibile e che siano stati rispettati i principi del procedimento. Il provvedimento adottato con il supporto di un sistema di IA è soggetto a tutti i vizi tradizionali — violazione di legge, incompetenza, eccesso di potere — più alcuni vizi specifici

riconducibili alle peculiarità del modulo algoritmico: opacità della logica, vizi di costruzione dell'algoritmo, distorsioni dei dataset di addestramento, mancata sorveglianza umana effettiva. Sono vizi sostanziali, non meramente formali, e il loro accertamento può portare all'annullamento del provvedimento secondo le ordinarie regole del processo amministrativo.

Il quarto profilo, di natura più sostanziale, concerne il diritto di non essere sottoposti a decisioni automatizzate ai sensi dell'articolo 22 del GDPR. Pur con le eccezioni che la disposizione prevede, e fermo restando il regime delle deroghe, il principio resta: una decisione che produca effetti giuridici o incida significativamente sulla persona non può essere il prodotto del solo trattamento automatizzato. La pubblica amministrazione che invochi una delle eccezioni — tipicamente quella dell'autorizzazione del diritto dell'Unione o dello Stato membro — è tenuta a fornire al cittadino le tutele che il paragrafo 3 della medesima disposizione prevede: il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di contestare la decisione. L'articolo 14 della legge 132/2025, nel rendere l'IA strumentale e di supporto al provvedimento, rinforza questa tutela sul versante interno: non si tratta solo di un diritto del cittadino, ma di un dovere oggettivo dell'amministrazione.

L'effettività di queste tutele dipende, come sempre, da fattori esterni alla norma. Dipende dalla capacità delle amministrazioni di rendere effettivamente conoscibili gli algoritmi che utilizzano, dalla qualità della motivazione, dalla disponibilità di canali di accesso agevoli, dalla competenza tecnica degli organi giudicanti chiamati a valutare la legittimità delle decisioni assistite. È un campo in cui la prossima legislatura, e in particolare l'opera del Governo nell'esercizio della delega di cui all'articolo 24 della legge 132/2025, sarà chiamata a fornire ulteriori specificazioni operative. Il quadro è già adesso sufficientemente ricco da consentire al cittadino di reagire a decisioni amministrative algoritmiche che non rispettino i parametri di legittimità: ne va incoraggiata l'effettività, e a questo concorrono tanto l'opera dei giudici quanto la cultura professionale dell'avvocatura amministrativa.

PROFILI OPERATIVI

Sette cantieri per chi gestisce la conformità

Mappatura, classificazione del rischio, valutazioni d'impatto, governance, appalti, formazione, coordinamento

Il passaggio dalle norme alle pratiche richiede, in ogni ente pubblico che intenda introdurre o stia già utilizzando sistemi di intelligenza artificiale, una progettazione organizzativa che faccia perno su alcune figure chiave e su alcuni processi che è bene avviare con metodicità. Il presente contributo si limita a indicare i nodi essenziali, senza pretesa di esaustività e tenendo conto del fatto che le specificità organizzative dei diversi enti — dal piccolo comune alla regione, dal ministero all'agenzia — richiederanno calibrazioni proprie.

Il primo nodo è la mappatura dei sistemi di IA già in uso o in fase di acquisizione. È un'attività che molti enti hanno avviato, in modo formalmente strutturato o informale, ma che spesso si scontra con la difficoltà oggettiva di qualificare come «sistema di IA» strumenti software che il fornitore o l'amministrazione non hanno presentato in tali termini. La definizione contenuta nell'articolo 3, paragrafo 1, del Regolamento (UE) 2024/1689 è il punto di riferimento: un sistema basato su macchine, progettato per funzionare con livelli di autonomia variabili, che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input ricevuto come generare output (previsioni, contenuti, raccomandazioni o decisioni) che possono influenzare ambienti fisici o virtuali. La definizione esclude i sistemi basati sulle sole regole definite da persone fisiche per eseguire operazioni automatiche; include, viceversa, una larga parte degli strumenti di triage documentale, classificazione automatica delle istanze, supporto decisionale, riconoscimento di pattern, valutazione predittiva. La mappatura va effettuata sistema per sistema, indicando per ciascuno la finalità d'uso, l'ufficio responsabile, l'esposizione delle persone interessate, la classificazione del rischio.

Il secondo nodo è la classificazione del rischio. Per i sistemi mappati va effettuata la verifica della loro riconducibilità all'Allegato III, e in particolare alle categorie di interesse per la PA che il contributo dedicato al deployer ha richiamato. La classificazione comporta conseguenze operative immediate sotto il profilo degli obblighi: per i sistemi ad alto rischio scattano la sorveglianza umana strutturata, la conservazione dei log, l'obbligo di FRIA, l'eventuale registrazione nella banca dati UE, gli obblighi informativi verso le persone interessate e, nei contesti lavorativi, verso i rappresentanti dei lavoratori. Per i sistemi non classificabili come ad alto rischio, restano comunque applicabili le tutele generali del GDPR (qualora vi sia trattamento di dati personali) e, in caso di interazione con persone fisiche o di generazione di contenuti, gli obblighi di trasparenza dell'articolo 50 dell'AI Act.

Il terzo nodo è la valutazione d'impatto. Va impostata, ove necessaria, sia la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35 del GDPR, sia la valutazione d'impatto sui diritti fondamentali di cui all'articolo 27 del Regolamento (UE) 2024/1689. Il raccordo tra le due, espressamente previsto dal paragrafo 4 dell'articolo 27, consente di costruire un unico processo valutativo modulare che, su uno stesso sistema, copra entrambi i profili senza duplicazioni inutili. La buona pratica è di partire dalla DPIA, già metodologicamente nota nelle amministrazioni che hanno strutture di protezione dei dati funzionanti, e di integrarla con i contenuti specifici della FRIA: identificazione delle categorie di persone interessate, dei rischi specifici di pregiudizio per i diritti fondamentali, delle misure di sorveglianza umana, dei meccanismi di governance interna. La FRIA è un documento vivo, da aggiornare ogniqualvolta cambino le condizioni d'uso del sistema.

Il quarto nodo è la governance interna. La distribuzione delle responsabilità tra le diverse figure del management pubblico va definita con precisione. Il Responsabile della transizione digitale, previsto dall'articolo 17 del Codice dell'amministrazione digitale, è la figura naturalmente competente per il coordinamento dei progetti di innovazione tecnologica che coinvolgano sistemi di IA. Il Data Protection Officer, in tutti gli enti tenuti alla sua nomina, è

coinvolto sin dalla fase di progettazione per il presidio dei profili di protezione dei dati e per la conduzione della DPIA. Il Responsabile della prevenzione della corruzione e della trasparenza ha un ruolo specifico nei sistemi che incidono su procedimenti soggetti a particolari obblighi di trasparenza o esposti a rischi corruttivi. La dirigenza apicale ha la responsabilità di assicurare che le decisioni strategiche sull'introduzione dei sistemi siano assunte con piena consapevolezza dei loro effetti, e che la sorveglianza umana effettiva sia organizzativamente garantita.

Il quinto nodo è quello degli appalti e dei contratti con i fornitori. La PA acquisisce sistemi di IA sul mercato; la qualità della relazione contrattuale determina in misura rilevante la possibilità di rispettare gli obblighi normativi. I capitolati tecnici e i contratti devono prevedere clausole specifiche sulla documentazione tecnica fornita dal produttore, sui requisiti di trasparenza, sulla disponibilità delle informazioni necessarie a effettuare la FRIA, sull'accesso alle informazioni occorrenti per esercitare la sorveglianza umana, sui livelli di servizio, sulla responsabilità in caso di malfunzionamenti, sulle modalità di aggiornamento e versionamento del sistema, sulla portabilità in caso di cessazione del rapporto. Per i sistemi ad alto rischio è opportuno che il contratto preveda esplicitamente la fornitura, da parte del produttore, della documentazione necessaria al deployer per assolvere ai propri obblighi dell'articolo 26 del Regolamento.

Il sesto nodo è la formazione del personale. L'obbligo di alfabetizzazione in materia di IA, mantenuto dall'articolo 4 del Regolamento per i sistemi ad alto rischio, va declinato in piani formativi differenziati per il personale che utilizza direttamente i sistemi, per quello che esercita la sorveglianza umana, per il personale di supporto e per il management. La formazione non si esaurisce in una sessione introduttiva: richiede aggiornamento periodico, dimensionato sull'evoluzione dei sistemi e sull'esperienza maturata nell'uso. Per le amministrazioni di minori dimensioni che non dispongono di strutture formative interne, il ricorso a percorsi consorziati o offerti dalle scuole della pubblica amministrazione è una via percorribile e raccomandabile.

Il settimo nodo, che è insieme cornice e premessa di tutti gli altri, è il coordinamento con il quadro nazionale italiano. L'articolo 20 della legge 132/2025 ha designato AgID come autorità di notifica e ACN come autorità di vigilanza del mercato, ferme restando le competenze del Garante per la protezione dei dati personali, dell'AGCOM, e — nei settori finanziari — di Banca d'Italia, CONSOB e IVASS. La PA che pianifica oggi l'introduzione di sistemi di IA si interfaccerà progressivamente con tutte queste autorità, ciascuna per la propria competenza. Per il DPO che opera nell'ente pubblico, il monitoraggio congiunto del doppio binario — europeo e nazionale — sarà attività ordinaria nei prossimi diciotto mesi, in vista della maturazione del quadro attuativo della legge 132/2025 entro il 10 ottobre 2026.

CONTRIBUTO SPECIALISTICO

[Titolo da definire]

In corso di pubblicazione

Sezione riservata al contributo specialistico

Questo spazio è destinato a un contributo specialistico in corso di pubblicazione, firmato da una studiosa che si unirà al fascicolo. Il contributo sarà integrato nella versione definitiva del numero al momento della sua ricezione.

Direzione scientifica · Centro Studi Innova Jus

PROSPETTIVE

Tre linee di sviluppo per i prossimi diciotto mesi

Decreti delegati, consolidamento del Digital Omnibus, evoluzione giurisprudenziale

Il numero che si chiude offre una fotografia in movimento. Il quadro normativo che disciplina l'uso dell'intelligenza artificiale da parte della pubblica amministrazione è oggi più ricco e più articolato di quanto fosse anche soltanto due anni fa, ma è tutt'altro che assestato. Tre linee di sviluppo segneranno i prossimi diciotto mesi, e meritano un'attenta osservazione da parte degli operatori.

La prima linea di sviluppo è interna all'ordinamento italiano: l'esercizio della delega contenuta nell'articolo 24 della legge 23 settembre 2025, n. 132. Il Governo è chiamato ad adottare, entro dodici mesi dall'entrata in vigore della legge — quindi entro il 10 ottobre 2026 — uno o più decreti legislativi per l'adeguamento della normativa nazionale al Regolamento (UE) 2024/1689 e per specificare la disciplina dei casi di realizzazione e impiego illeciti di sistemi di intelligenza artificiale. È prevista, inoltre, una delega specifica per la definizione di una disciplina organica dell'utilizzo di dati, algoritmi e metodi matematici per l'addestramento dei sistemi, negli ambiti soggetti al Regolamento europeo. Gli schemi dei decreti sono adottati su proposta del Presidente del Consiglio dei ministri e del Ministro della giustizia, trasmessi alle Camere per il parere delle commissioni competenti; decorsi sessanta giorni dalla trasmissione, possono essere emanati anche in mancanza dei pareri. Per la pubblica amministrazione, i decreti delegati sono il prossimo orizzonte in cui sarà specificata, presumibilmente, parte rilevante dell'apparato sanzionatorio, della governance del rischio e dei profili attuativi.

La seconda linea di sviluppo è sovranazionale: il consolidamento del Digital Omnibus on AI, sul quale il primo numero di questa rivista ha offerto un'analisi articolata. L'accordo politico provvisorio del 7 maggio 2026, che ha fissato le nuove scadenze applicative degli obblighi sui sistemi ad alto rischio (2 dicembre 2027 per i sistemi dell'Allegato III, 2 agosto 2028 per quelli incorporati nei prodotti dell'Allegato I), richiede ancora il voto formale di Parlamento e Consiglio e la revisione giuridico-linguistica prima della pubblicazione in Gazzetta Ufficiale dell'Unione europea. Entrambe le istituzioni hanno dichiarato l'intenzione di completare l'adozione prima del 2 agosto 2026. Per la PA italiana, la cui scadenza applicativa di gran parte degli obblighi del Capo III del Regolamento si sposta al 2 dicembre 2027, l'orizzonte di pianificazione è dunque più ampio di quanto era stato originariamente previsto, ma non infinito: meno di venti mesi alla data di chiusura del presente fascicolo. È un orizzonte sufficiente per costruire un'effettiva conformità, non sufficiente per attendere ulteriori rinvii.

La terza linea di sviluppo è giurisprudenziale, e attiene al consolidamento dell'orientamento del Consiglio di Stato sull'algoritmo amministrativo. La trilogia 2270/2019 — 8472/2019 — 881/2020 ha fissato i principi cardine; la giurisprudenza successiva, anche di primo grado, ha cominciato a confrontarsi con casi più complessi e con tipologie di sistema diverse da quelle del concorso docenti che fu all'origine della prima pronuncia. L'interazione tra i principi consolidati e i nuovi obblighi del Regolamento (UE) 2024/1689 produrrà, prevedibilmente, ulteriori specificazioni giurisprudenziali, in particolare sui temi della FRIA, della responsabilità del deployer pubblico, della sorveglianza umana effettiva, della motivazione del provvedimento adottato con il supporto algoritmico. La Corte di giustizia, per parte sua, dopo la sentenza SCHUFA Holding del dicembre 2023 (causa C-634/21) e la sentenza Dun & Bradstreet Austria del febbraio 2025 (causa C-203/22), sta costruendo un proprio corpus sull'interpretazione dell'articolo 22 del GDPR. La convergenza tra giurisprudenza europea e giurisprudenza amministrativa nazionale è un fenomeno che merita osservazione attenta nei prossimi mesi.

Una considerazione finale di natura più ampia. Il modello di amministrazione algoritmica che il nostro ordinamento sta costruendo non corrisponde — e non deve corrispondere — a un modello di sostituzione della decisione umana con la decisione automatizzata. È, piuttosto, un modello di integrazione strumentale, in cui l'IA assiste la formazione

del provvedimento amministrativo senza sostituirsi all'organo titolare del potere, e in cui la responsabilità della decisione resta umana, sindacabile e comprensibile. È un modello impegnativo da realizzare nella pratica, perché richiede investimenti organizzativi e formativi che non si improvvisano. È, però, l'unico modello compatibile con i principi costituzionali, amministrativi e europei che governano l'azione pubblica. Per chi opera nella pubblica amministrazione italiana — dirigenti, funzionari, DPO, RTD, Responsabili anticorruzione, professionisti che le assistono — i prossimi due anni saranno il tempo in cui questo modello dovrà passare dalle enunciazioni alla pratica quotidiana. Il presente fascicolo ha cercato di offrire un contributo a questo passaggio.

RIFERIMENTI

Fonti primarie e atti istituzionali

Atti normativi, giurisprudenza e documenti consultati

Fonti normative

Costituzione della Repubblica italiana, art. 97 (principio di buon andamento e imparzialità dell'azione amministrativa).

Legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.

Decreto legislativo 7 marzo 2005, n. 82, recante il Codice dell'amministrazione digitale.

Decreto legislativo 14 marzo 2013, n. 33, recante il riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni.

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR), in GUUE L 119 del 4.5.2016.

Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (AI Act), in GUUE L del 12.7.2024.

Legge 23 settembre 2025, n. 132, recante disposizioni e deleghe al Governo in materia di intelligenza artificiale, in Gazzetta Ufficiale n. 223 del 25 settembre 2025; in vigore dal 10 ottobre 2025.

Giurisprudenza

Consiglio di Stato, sez. VI, 8 aprile 2019, n. 2270 (prima sentenza della trilogia sull'algoritmo amministrativo).

Consiglio di Stato, sez. VI, 13 dicembre 2019, n. 8472, Pres. Montedoro, Est. Ponte (e sentenze gemelle nn. 8473 e 8474 della stessa data).

Consiglio di Stato, sez. VI, 4 febbraio 2020, n. 881.

Corte di giustizia dell'Unione europea, Prima Sezione, sentenza del 7 dicembre 2023, SCHUFA Holding, causa C-634/21 (sulla qualificazione del scoring come decisione automatizzata ai sensi dell'art. 22 GDPR).

Corte di giustizia dell'Unione europea, Prima Sezione, sentenza del 27 febbraio 2025, Dun & Bradstreet Austria, causa C-203/22 (sul diritto a una spiegazione concreta della logica utilizzata nei processi decisionali automatizzati ex art. 15, par. 1, lett. h, del GDPR).

Atti istituzionali e documenti consultati

Commissione europea, comunicazione e atti istituzionali in materia di intelligenza artificiale; pacchetto Digital Omnibus (COM(2025) 836 e COM(2025) 837 final, 19 novembre 2025).

Parlamento europeo e Consiglio dell'Unione europea, comunicati relativi all'accordo politico provvisorio sul Digital Omnibus on AI del 7 maggio 2026.

EDPB-EDPS, Joint Opinion 1/2026 del 20 gennaio 2026 sul Digital Omnibus on AI; Joint Opinion 2/2026 dell'11 febbraio 2026 sul Digital Omnibus generale.

Agenzia per l'Italia Digitale (AgID) e **Agenzia per la cybersicurezza nazionale (ACN)**, atti e provvedimenti pubblicati nell'ambito delle rispettive competenze sulle materie qui trattate.

Conferenza Stato-Città ed autonomie locali, approfondimenti istituzionali sull'intelligenza artificiale nella pubblica amministrazione.

Avvertenza finale. Il presente fascicolo è chiuso alla data del 27 maggio 2026. L'esercizio della delega di cui all'articolo 24 della legge 132/2025 e il consolidamento formale del Digital Omnibus on AI potranno intervenire nei mesi successivi alla pubblicazione del numero e, ove incidano su singoli profili qui trattati, saranno oggetto di aggiornamento nei prossimi numeri della rivista.

INNOVA JUS — Rivista del Centro Studi · Anno I · Numero 2 · Giugno 2026 · Tema monografico: L'amministrazione algoritmica. · Direzione scientifica: Prof. Avv. Michele Iaselli. · innovajus.it